DePaul University
University Libraries

DePaul Law Review

Volume 66
Issue 4 *Summer 2017*

Article 6

An Uphill Battle: FTC Regulation of Unreasonable Data Security as an Unfair Practice

Nelly Rosenberg

AN UPHILL BATTLE: FTC REGULATION OF UNREASONABLE DATA SECURITY AS AN UNFAIR PRACTICE

INTRODUCTION

We live in a society permeated by technology.[1] Most households in the United States have internet access, and a majority of Americans regularly use two or more internet connected devices.[2] In 2016, there were over three billion internet users worldwide, and the number is projected to surpass three and a half billion in 2017.[3] The number of connected devices increased from 8.7 billion in 2012 to 22.9 billion in 2016, and it is projected to increase to 50.1 billion by 2020.[4] We spend our days switching from device to device checking email, using social media, shopping online, watching shows and movies, playing games, and myriad other things that the internet and modern technology allow us to do.[5] With every credit card purchase, every app download, every new account set-up, people allow businesses to track, gather, and use their information.[6] This information can include names, addresses, social security numbers, dates of birth, credit card informa-

1. Giulia McHenry, *Majority of Americans Use Multiple Internet-Connected Devices, Data Shows*, NAT'L TELECOMMS. & INFO. ADMIN. (Dec. 7, 2015), https://www.ntia.doc.gov/blog/2015/majority-americans-use-multiple-internet-connected-devices-data-shows.

2. *Id.*; *see also Measuring America: A Digital Nation*, U.S. CENSUS BUREAU (Mar. 23, 2016), https://www.census.gov/content/dam/Census/library/visualizations/2016/comm/digital_nation.pdf. This statistic is based on the 2014 American Community Survey conducted by the Census Bureau. *Id.*

3. *Internet Users*, INTERNET LIVE STATS, http://www.internetlivestats.com/internet-users/#trend (last visited Jan. 15, 2017).

4. *Internet of Things (IoT): Number of Connected Devices Worldwide from 2012 to 2020 (in Billions)*, STATISTA, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (last visited Jan. 15, 2017).

5. *See How Smartphones Are Changing Consumers' Daily Routines Around the Globe*, NIELSEN (Feb. 24, 2014), http://www.nielsen.com/us/en/insights/news/2014/how-smartphones-are-changing-consumers-daily-routines-around-the-globe.html.

6. *See 60 Minutes: The Data Brokers* (NBC television broadcast Aug. 24, 2014), http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/. In many instances, consumers are not even aware that their personal information is being gathered. *See* RSA, CONSUMER PERCEPTIONS ON SECURITY: DO THEY STILL CARE? (2014), https://www.emc.com/collateral/brochure/consumer-perceptions-on-security.pdf ("[O]nly about one-third of consumers admit to actually reading the permissions requested by the apps they download.").

tion, usernames and passwords, GPS location, and much more.[7] Consumers can be proactive in safeguarding their personal information;[8] however, the extent to which they can do so is limited because once consumers provide their personal information or allow it to be gathered, what happens to that data is out of their hands.[9] Consumers cannot control how their information is stored, so they place a great amount of trust in businesses and expect their information to be protected from unauthorized access.[10]

As waves of massive data breaches swept across American commercial and financial sectors,[11] people have become more concerned about the privacy and security of their personal information.[12] This increased concern is well-founded, as companies of different sizes across different industries continue to experience data breaches.[13] A few of the affected companies include JPMorgan Chase Bank, Amazon, Aon Hewitt, Comcast, Home Depot, Target, Neiman Marcus, T-Mobile, Sony, Hilton Worldwide, Uber, Trump Hotels, Costco, State Farm, American Airlines, and United Airlines, but the list goes on and on.[14]

Of course, not every data breach is preventable and not every breach leads to identity theft or fraudulent charges;[15] however, once

---

7. *See* Andrew McAfee & Erik Brynjolfsson, *Big Data: The Management Revolution*, HARV. BUS. REV. (Oct. 2012), https://hbr.org/2012/10/big-data-the-management-revolution.

8. *How to Keep Your Personal Information Secure*, FTC (July 2012), https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure.

9. *See generally* 2 PRIVACY IN THE INFORMATION SOCIETY (Philip Leith ed., 2015).

10. *See* RSA, *supra* note 6 ("While many consumers are doing minimal to change their behavior, they still place value in their personal information and have high expectations among service providers to secure their digital identities.").

11. *See* FTC, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY-DECEMBER 2014, at 3–5, 12 (2015), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.pdf.

12. *See* TRAVELERS INDEM. CO., CONSUMER RISK INDEX: AN ANNUAL SURVEY OF THE RISKS AMERICANS BELIEVE ARE MOST PREVALENT IN THEIR LIVES (2015), https://www.travelers.com/iw-documents/resources/consumer-risk-index/2015-report.pdf. According to a study performed by the Travelers Insurance Company on consumer perception of different types of risks, "[c]oncern over cyber, computer and tech-related risks rose sharply in 2015" with an increase from 36% in 2014 to 57% in 2015. *Id* at 2. The study further indicates that one in four people "surveyed say they have been a victim of a data breach or cyber attack." *Id*.

13. In this Comment, "data breach" refers to an incident when an unauthorized third party gains remote access to sensitive electronic information. This Comment does not address incidents when data was inadvertently disclosed through error or negligence or when physical files were copied or removed from company premises.

14. *See* IDENTITY THEFT RESOURCE CTR., DATA BREACH REPORTS (2015), http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf [hereinafter 2015 DATA BREACH REPORT].

15. *See* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 170 (2008); *see also Protecting*

personal information is obtained by an unauthorized party, there is always the risk that identity theft or fraudulent charges may occur. As Chief Judge Wood reasoned in *Remijas v. Neiman Marcus Group, LLC*,[16] a class action suit arising out of hackers obtaining customer credit card information, "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[17] Despite the fact that data breaches affect millions of consumers, individuals have little legal or economic recourse.

A patchwork of regulation has developed in response to the growing need for oversight of information security practices across different industries. Courts have granted relief only to consumers who can quantify harm arising out of a data breach—generally due to identity theft or fraudulent charges.[18] Congress has reviewed numerous proposed bills for regulation of information security on a national level.[19] Almost all states passed data breach notification laws, which require certain entities to disclose data breaches and notify affected consumers.[20] Administrative agencies have released industry specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule for the healthcare sector[21] and the Gramm-Leach-Bliley Act of 1999 (GLBA) covering financial institutions,[22]

Our Nation's Cyber Space: Educational Awareness for the Cyber Citizen: Hearing Before the H. Subcomm. on Tech., Info. Pol'y, Intergovernmental Relations & the Census, Comm. on Gov't Reform, 108th Cong. 5 (2004) (prepared statement of the Fed. Trade Comm'n), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-our-nations-cyberspace/042104cybersecuritytestimony.pdf [hereinafter *FTC Statement*].

16. 794 F.3d 688 (7th Cir. 2015).

17. *Id.* at 693.

18. *See id*. at 692 ("These plaintiffs must allege that the data breach inflicted concrete, particularized injury on them.").

19. *See Current Legislation*, CONGRESS.GOV, https://www.congress.gov/ (select "Current Legislation" next to search bar and search for "information security") (last visited Mar. 13, 2017); *see also* ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW OF MAJOR ISSUES, CURRENT LAWS, AND PROPOSED LEGISLATION (2014), https://fas.org/sgp/crs/natsec/R42114.pdf.

20. *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGIS. (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx ("Forty-eight states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.").

21. *See Covered Entities and Business Associates*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Jan. 15, 2017); *see also* GINA STEVENS, CONG. RESEARCH SERV., RL34120, FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS 10 (2010), https://www.fas.org/sgp/crs/secrecy/RL34120.pdf.

22. *See* STEVENS, *supra* note 21, at 17.

among others. Within this patchwork, certain business entities are still not subject to any regulation outside the state data breach notification laws. The need for more comprehensive regulation of information security grows while gaps in such a regulation still exist.[23]

In response to the growing need for oversight, the Federal Trade Commission (FTC) has taken on a dominant role in data security regulation of the business entities subject to its jurisdiction.[24] The FTC seeks to promote competition and protect consumers by "stopping unfair, deceptive or fraudulent practices in the marketplace."[25] The FTC has the power to conduct investigations, enforce regulations through administrative adjudication, and promulgate trade regulation rules (TRRs).[26] In the data security context, the FTC considers inadequate information security practices as unfair or deceptive practices prohibited by the Federal Trade Commission Act (FTCA).[27] Between 2002 and 2016, the FTC successfully settled over sixty enforcement actions against companies with inadequate information security.[28] Considering the escalating number of new data breaches, pursuing individual companies on a case-by-case basis is not an efficient means of effectuating change in the marketplace.

The FTC proclaims its mission is to prevent substantial consumer harm.[29] In today's landscape of recurrent data breaches, consumers are harmed by unauthorized access to their personal and financial information. This may be due to identity theft, fraudulent charges, or paying for services to monitor for identity theft and fraudulent charges. The best way to protect consumers from harm caused by data breaches is to reduce the occurrence of data breaches in the com-

23. *Prepared Statement of the Federal Trade Commission* 1–2 (2014), https://www.ftc.gov/system/files/documents/public_statements/630961/150318datasecurity.pdf. PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION on Discussion Draft of H.R.__, Data Security and Breach Notification Act of 2015 Before the COMMITTEE ON ENERGY AND COMMERCE SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE UNITED STATES HOUSE OF REPRESENTATIVES Washington, D.C. March 18, 2014

24. *See* David J. Bender, *Tipping the Scales: Judicial Encouragement of a Legislative Answer to FTC Authority over Corporate Data-Security Practices*, 81 GEO. WASH. L. REV. 1665, 1674 (2013).

25. *See* 15 U.S.C. §§ 45(a), 45(n), 57a (2012); *About the FTC: What We Do*, FTC, https://www.ftc.gov/about-ftc/what-we-do (last visited Jan. 15, 2017).

26. *See* 15 U.S.C. §§ 45(a), 45(n), 57a; *see also* Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 997 (2016) (noting that although the FTC has clear rulemaking authority, "the FTC consistently relies on adjudication over rulemaking").

27. 15 U.S.C. §§ 41–58 (2012).

28. FTC, PRIVACY & DATA SECURITY UPDATE: 2016 4 (2017), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf [hereinafter DATA SECURITY UPDATE].

29. *See About the Federal Trade Commission*, FTC, https://www.ftc.gov/about-ftc (last visited Mar. 5, 2016) [hereinafter *About the FTC*].

mercial sector. To safeguard against data breaches, companies must be required to implement an information security program tailored to protect that company's electronically stores files. Although what constitutes a reasonable data security program is specific to each company, there are basic precautionary measures and general guidelines that every company should follow to reduce the risk of data breaches. The FTC has released numerous guides about suggested information security practices for companies to consider, but no mandatory standard currently exists.

The FTC has been successful in its past enforcement actions in the area of privacy and data security, but there are few such cases compared to the number of companies that recently suffered data breaches due to inadequate information security practices. Critics claim that the FTC has exceeded its authority under the FTCA,[30] and two companies have already challenged the FTC's authority to regulate inadequate information security as an unfair practice.[31] The FTC has a long way to go before it can regulate commercial data security on a level that will have a positive impact on the marketplace. The FTC's inability to regulate unreasonable data security measures on a larger scale significantly undermines its efforts to prevent substantial consumer injury. This Comment argues that the FTC should promulgate a TRR that articulates minimum information security standards. The FTC has been reluctant to promulgate TRRs in fear that such rules would become obsolete in the face of developing technology.[32] Such fears prevent the FTC from regulating information security in the commercial sector effectively and efficiently.

Part II of this Comment surveys the current landscape of data security and its regulation, including statistics concerning frequency and scope of recent data breaches, legislative approaches to regulation of data security, and the FTC's evolving role in the data security context.[33] Part III of this Comment examines the challenges the FTC faces in proving the elements of unfair or deceptive practices claim under section 45(a) of the FTCA.[34] This Part demonstrates how, ab-

30. *See, e.g.*, Gerard M. Stegmaier & Wendell Bartnick, *Essay, Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 691–93 (2013).

31. *See* Amanda R. Moncada, Comment: *When a Data Breach Comes A-Knockin', the FTC Comes A-Blockin': Extending the FTC's Authority to Cover Data-Security Breaches*, 64 DEPAUL L. REV. 911, 921–24; *see also infra* notes 112–70 and accompanying text.

32. *See* Hurwitz, *supra* note 26, at 154 ("It is unsurprising, then, that [areas defined by new or changing technologies] are the areas in which we see the FTC pushing aggressively to rely on adjudication and characterizing its efforts as akin to 'common law.'").

33. *See infra* notes 36–170 and accompanying text.

34. *See infra* notes 176–304 and accompanying text.

sent a TRR that expressly grants the FTC the authority to regulate information security practices, the FTC lacks a streamlined manner of enforcement, which significantly limits its ability to regulate information security. If an entity does not voluntarily settle, then the FTC must prove every element of the "unfair" practice in each and every case, as defined by the FTCA. Part IV examines the impact of recent federal and administrative decisions on the future enforcement actions, as well as the likely consequences if the FTC continues to rely on case-by-case adjudication.[35] Part V concludes by discussing the likelihood of the FTC promulgating a TRR and the outlook of FTC's future enforcement actions.

II. BACKGROUND

The number of data breaches is continuously escalating.[36] Despite this prevalent threat, the United States does not have comprehensive legislation to address this issue.[37] Instead, Congress, state governments, and administrative agencies have created a "patchwork" of legislation and regulations that cover certain entities, including healthcare providers, financial institutions, and government agencies.[38] This piecemeal regulation, however, does not cover a significant portion of business entities. In light of this deficiency, the FTC stepped up as the primary enforcer of data security in the business sector.[39] The FTC has been successful in its enforcement actions arising from inadequate information security; however, these cases ended in settlement, and the FTC will face challenges to its authority,[40] as it has already in the cases of *FTC v. Wyndham Worldwide Corp.*[41] and *LabMD, Inc. v. FTC*.[42]

Section A provides statistics about of the number of occurrences and types of data breaches that have occurred in the recent years. Section B then explores the current state of information security regulation. Finally, Section C discusses the FTC's evolving role in information security regulation.

---

35. *See infra* notes 305–29 and accompanying text.
36. *See infra* notes 43–54 and accompanying text.
37. *See infra* notes 72–76 and accompanying text.
38. *See infra* notes 72–76 and accompanying text.
39. *See* Scott, *supra* note 15, at 128–29.
40. DATA SECURITY UPDATE, *supra* note 28; *see also* Suevon Lee, *D-Link Fires Back at FTC's Lax Data Security Claims*, LAW360 (Jan. 31, 2017, 9:04 P.M.), https://www.law360.com/articles/887031/d-link-fires-back-at-ftc-s-lax-data-security-claims (discussing D-Link's assertion that the FTC overstepped its authority under section 5 of the FTCA).
41. 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).
42. No. 16-16270-D, 2016 FTC LEXIS 123 (F.T.C. July 28, 2016), *stay granted*, LabMD, Inc. v. FTC, No. 16-16270-D, 2016 U.S. App. LEXIS 23559 (11th Cir. Nov. 10, 2016).

A. Data Breach Statistics

Incidents of data breaches are increasing, and hackers have gained access to hundreds of millions of consumer records.[43] The Identity Theft Resource Center (ITRC) collects statistics on the instances of data breaches across various industries, including business, medical, government, educational, and financial industries.[44] The ITRC defines a breach as "an incident in which an individual name plus Social Security Number, driver's license number, medical record or a financial record (credit/debit cards included) is potentially put at risk."[45] According to ITRC, the business sector suffered the largest number of data breach incidents in 2016.[46] A summary of ITRC's findings from 2005 to 2016 is illustrated in Figure 1.[47]

43. FTC, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY-DECEMBER 2015, at 4 (2016), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf.

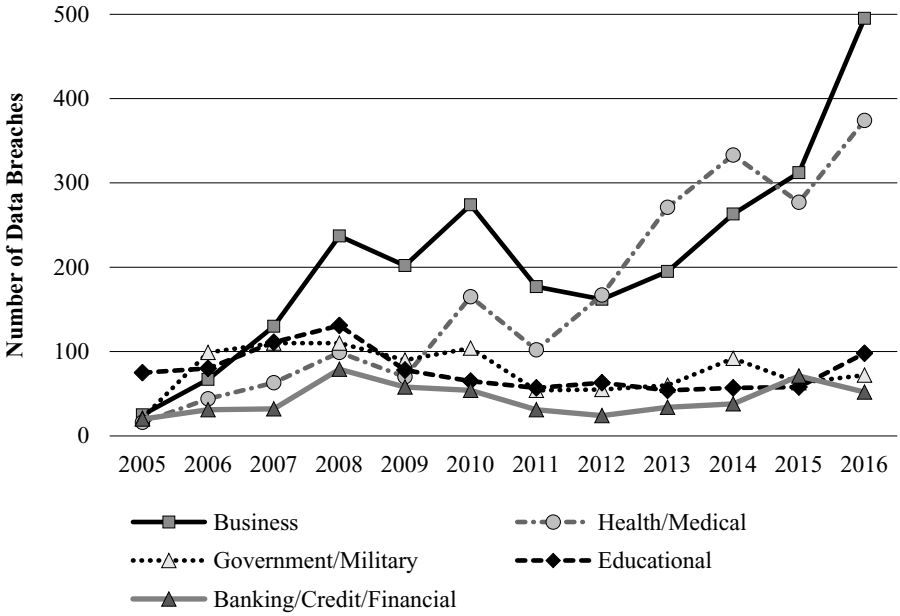
44. The ITRC provides free assistance to victims of fraud and identity theft and conducts research and surveys to "[e]ducate consumers, corporations, government agencies, and other organizations on best practices for fraud and identity theft detection, reduction and mitigation." *Our Mission*, IDENTITY THEFT RESOURCE CTR., http://www.idtheftcenter.org/About-ITRC/about-us.html (last visited Mar. 4, 2016).

45. 2015 DATA BREACH REPORT, *supra* note 14.

46. *See* IDENTITY THEFT RESOURCE CTR., DATA BREACH REPORTS: 2016 END OF THE YEAR REPORT (2017), http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf [hereinafter 2016 DATA BREACH REPORT]; *see also* IDENTITY THEFT RESOURCE CTR., ITRC BREACH STATISTICS 2005–2016 (2017), http://www.idtheftcenter.org/images/breach/2016/2005to2016.pdf [hereinafter ITRC BREACH STATISTICS].

47. *See* ITRC BREACH STATISTICS, *supra* note 46.

FIGURE 1: DATA BREACH INCIDENTS BY CATEGORY



In 2016, there were 1093 data breaches, which is a 40% increase from 780 breaches in 2015.[48] Businesses that experienced a data breach in the past few years include Yahoo, Amazon, Hyatt Hotels, Safeway, Kohl's, Aon Hewitt, Comcast, Uber, T-Mobile, Trump Hotels, Costco, State Farm, Esurance, Wendy's, American Airlines, and United Airlines, among many others.[49] Statistics also show an increase in data breaches due to hacking.[50] The ITRC reported that "[i]n 2015, Hacking incidents reached a nine-year high of 37.9 percent, a jump of 8.4 percent over 2014 figures."[51] The number of hacking

48. *See* 2015 DATA BREACH REPORT, *supra* note 14. The ITRC also tracks the number of records released, but it is only an estimate as the actual number of released records is unknown. *See id.* at 3. The number of known compromised records is affected by the reporting requirements imposed upon entities which experienced a data breach. *See generally Security Breach Notification Laws*, *supra* note 20. Each state has its own requirements for disclosure and notification under the data breach notification laws, so the number of known records released varies based on each state's unique reporting requirements. *Id.* Additionally, the healthcare sector is required to report data breach incidents under HIPAA and the FTC's Health Data Breach Notification law. *See* FTC, FTC FACTS FOR BUSINESS: COMPLYING WITH THE FTC'S HEALTH BREACH NOTIFICATION RULE (2010), https://www.ftc.gov/system/files/documents/plain-language/bus56-complying-ftcs-health-breach-notification-rule.pdf.

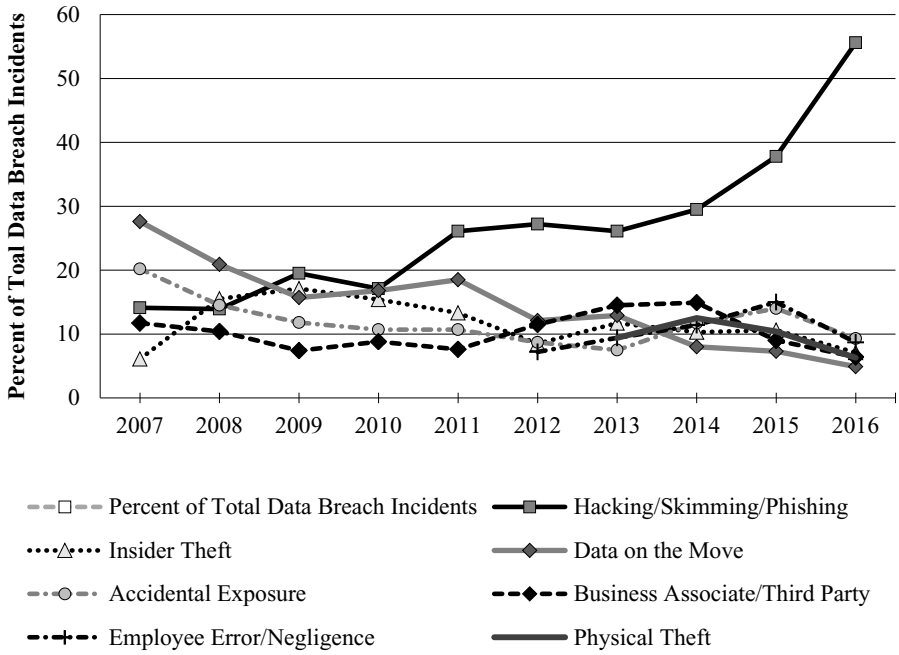
49. *See* 2015 DATA BREACH REPORT, *supra* note 14; 2016 DATA BREACH REPORT, *supra* note 46.

50. *See* ITRC BREACH STATISTICS, *supra* note 46.

51. *See Identity Theft Resource Center Breach Report Hits Near Record High in 2015*, IDENTITY THEFT RESOURCE CTR. (Jan. 25, 2016) http://www.idtheftcenter.org/ITRC-Surveys-Studies/

incidents increased again in 2016, reaching 55.6% of all data breach incidents. Figure 2 illustrates the percentages of data breaches due to different causes.[52]

FIGURE 2: DATA BREACH INCIDENTS BY TYPE



According to Adam Levin, Chairman and Founder of IDT911, one of the sponsors of IDRC that offers breach mitigation and identity management services,

> These numbers are by no means the whole story, as breaches have become the third certainty in life . . . . Many continue to fly under the radar because many businesses aim to avoid the financial dislocation, liability, and loss of goodwill that comes with disclosure and notification . . . . It is safe to assume that the actual number of breaches is much higher than what is reported.[53]

2015databreaches.html [hereinafter *Record High in 2015*]. The ITRC uses seven categories to classify data breaches: "Insider Theft, Hacking, Data on the Move, Subcontractor/Third Party, Employee error/negligence, Accidental web/ Internet Exposure and Physical Theft." 2015 DATA BREACH REPORT, *supra* note 14, at 2.

52. *See* ITRC BREACH STATISTICS, *supra* note 46.

53. *Record High in 2015*, *supra* note 51; *see also* Stegmaier & Bartnick, *supra* note 30, at 673–674 ("Most states require entities to notify affected individuals when certain personal information is affected by a breach.").

Although not every data breach is preventable and not every data breach results in identity theft,[54] the frequency of data breaches is alarming and further emphasizes the need to reform the current state of information security regulation.

B. Current State of Data Security Regulation

Information security is regulated by a patchwork of laws and regulations. The judicial system, federal and state law, and various administrative agencies each offer limited regulation.

1. Judicial System

Consumers who brought civil suits against companies following data breaches have seen limited success.[55] The judicial system provides recourse to individuals who can prove actual harm and establish standing under Article III of the Constitution.[56] Those who suffered identity theft or fraudulent charges that resulted in quantifiable monetary losses can establish actual harm; however, the consumers whose information was released in a data breach but who cannot show quantifiable losses could not satisfy Article III standing.[57] In *Clapper v. Amnesty Int'l USA*,[58] the Supreme Court held that a plaintiff alleging future harm from a defendant's improper conduct must establish that the harm is "certainly impending."[59] In *Remijas v. Neiman Marcus Group, LLC*, the Seventh Circuit Court of Appeals applied this standard in the data breach context and overturned the district court's dismissal of the class action suit for lack of standing under Article III.[60] The Circuit Court held that "[a]llegations of future harm can establish Article III standing if that harm is 'certainly impending,'" but the court did limit this threshold by including that "allegations of possible future injury are not sufficient."[61] The *Remijas* holding gives litigants in the Seventh Circuit a better chance to bring a claim; how-

54. *See* Scott, *supra* note 15, at 170; *see also FTC Statement*, *supra* note 15, at 5 ("Although a breach may indicate a problem with a company's security, breaches can happen . . . even when a company has taken every reasonable precaution.").

55. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690–92 (7th Cir. 2015) (discussing the requirements to meet standing under Article III of the Constitution).

56. *Id.* at 692 ("These plaintiffs must allege that the data breach inflicted concrete, particularized injury on them."); *see also* Scott, *supra* note 15, at 155 ("In the identity theft context, courts have embraced the general rule that an alleged increase in risk of future injury is not an 'actual or imminent injury.'" (quoting Key v. DSW, Inc., 454 F. Supp. 2d 684, 689 (S.D. Ohio 2006)).

57. *See Remijas*, 794 F.3d at 692, 696.

58. 133 S. Ct. 1138 (2013).

59. *Id*. at 1143.

60. *See Remijas*, 794 F.3d at 697.

61. *See id.* at 692 (quoting *Clapper*, 133 S. Ct. at 1147).

ever, the case has not been decided on the merits, so it is still to be determined whether individuals whose information was obtained in a data breach can recover damages without suffering actual, quantifiable harm.[62]

2. *State Laws*

State laws similarly offer limited protection to consumers because they focus on disclosure and remediation after a data breach has already occurred.[63] Forty-eight states passed their own variation of a data breach notification law, which requires certain entities to disclose certain instances of data breaches and to timely notify those affected by the breach.[64] Notification following a data breach is important for the mitigation process; however, it does not resolve the underlying issue that a data breach has occurred.[65]

Requirements across states are not uniform, including the entities that must report data breaches, the types of breaches that entities must report, and the time frame to notify the affected consumers.[66] In the majority of states, after a data breach, a company must notify the affected consumer "in the most expedient time possible and without unreasonable delay."[67] In nine states, however, the statute provides a definite time limit for notice (e.g., forty-five days).[68]

Until recently, all the states with a data breach notification law provided an exception for encrypted information.[69] Tennessee was the first state to amend the definition of a "breach of the security of the system" requiring notice in cases of unauthorized access to encrypted information.[70] Additionally, fifteen states provide for a private cause of action for violations of the breach notification statutes.[71]

---

62. *See id.* at 697.

63. *See generally Security Breach Notification Laws*, *supra* note 20.

64. *See id.*

65. *See id.*; *see also* Michael Keller, *Holiday Shopping? How Much Do Data Breach Notification Laws Protect?*, AL JAZEERA ENGLISH (Dec. 1, 2014, 5:00 AM), http://america.aljazeera.com/multimedia/2014/12/to-catch-a-breachhowmuchdodatabreachnotificationlawsprotect.html.

66. *See Security Breach Notification Laws*, *supra* note 20.

67. Stephen Embry, *State Data Breach Notification Laws Just Got Crazier*, ABA (May 2016) http://www.americanbar.org/publications/youraba/2016/may-2016/state-data-breach-notification-laws-just-got-crazier.html; *see, e.g.*, 815 ILL. COMP. STAT. 530/10 (2014 & Supp. 2016).

68. Embry, *supra* note 67 ("Five states—Ohio, Rhode Island, Vermont, Washington and Wisconsin—have a 45-day period.").

69. *Id.*; *see, e.g.*, 815 ILL. COMP. STAT. 530/5 (2014 & Supp. 2016).

70. TENN. CODE ANN. § 47-18-2107 (2016); Embry, *supra* note 67.

71. Embry, *supra* note 67.

3. Federal Law

Congress reviewed dozens of proposed bills concerning broad oversight of privacy and data security, but has not yet passed any comprehensive laws.[72] Instead, Congress passed legislation targeted at particular industries and conferred authority on administrative agencies to enforce the regulations.[73] For example, the HIPAA Privacy Rule establishes national standards to protect medical records and other personal health information for covered entities, including health care providers, health plans, health care clearinghouses, and related entities.[74] The GLBA requires financial institutions to protect consumers' private information from unauthorized access and to provide customers with notice of their privacy policies.[75] The financial sector must comply with the Safeguards Rule under the GLBA, which requires financial institutions to ensure safety and confidentiality of sensitive consumer information.[76]

There are numerous proposed bills currently before Congress that seek to require business entities to implement an information security program.[77] A few of the proposed bills particularly charge the FTC with implementing and administrating a framework to regulate data security.[78] For example, the Data Security Act of 2015 proposes to "establish strong and uniform national data security and breach notification standards for electronic data" and "to provide the Federal Trade Commission with authority to enforce such standards."[79] The Consumer Privacy Protection Act of 2015 seeks to require certain entities to comply with the listed safeguards and charges the FTC to enforce compliance in addition to any "safeguards identified by the Federal Trade Commission in a rulemaking process."[80] Under the Commercial Privacy Bill of Rights Act of 2015, the FTC would be directed to "initiate a rulemaking proceeding to require each covered entity [that collects or uses information about individuals] to carry out

72. *See Current Legislation*, *supra* note 19.

73. *See Covered Entities and Business Associates*, *supra* note 21; s*ee also* STEVENS, *supra* note 21, at 10.

74. *See Covered Entities and Business Associates*, *supra* note 21.

75. *See also* STEVENS, *supra* note 21, at 17.

76. *See* FTC, SAFEGUARDING CUSTOMERS' PERSONAL INFORMATION: A REQUIREMENT FOR FINANCIAL INSTITUTIONS (2002), https://www.ftc.gov/system/files/documents/plain-language/alt115-safeguarding-customers-personal-information-requirement-financial-institutions.pdf.

77. *See, e.g.*, Commercial Privacy Bill of Rights Act of 2015, H.R. 1053, 114th Cong. (1st Sess. 2015); Data Security Act of 2015, H.R. 2205, 114th Cong. (1st Sess. 2015); Consumer Privacy Protection Act of 2015, S. 1158, 114th Cong. (1st Sess. 2015).

78. *See, e.g.*, H.R. 1053; S. 1158.

79. H.R. 2205, § 2.

80. S 1158, at 17.

security measures to protect [personally identifiable information] it collects and maintains."[81] The abundance of proposed bills regarding information security regulation by the FTC demonstrates the legislature's desire to prevent data breaches in the commercial sector, as opposed to notification and mitigation after a breach has already occurred, and the FTC is in the best position to actively regulate information security practices.

4. Administrative Agencies

Administrative agencies have focused on data security issues within their respective jurisdictions, including the FTC, Department of Justice (DOJ), Department of Homeland Security (DHS), Securities and Exchange Commission (SEC), Federal Communications Commission (SEC), the Financial Industry Regulatory Authority (FINRA), and the Consumer Financial Protection Bureau (CFPB).[82]

Prior to 2000, the commercial sector was essentially self-regulating with respect to the level of security implemented to safeguard sensitive information.[83] Companies voluntarily promised to their customers a certain level of privacy and information security.[84] The FTC first began to intervene when companies failed to deliver on their own promises and then expanded its scope of enforcement to include companies that lacked sufficient information security measures.[85]

C. Evolution of Data Security Regulation by the FTC

To fill the void in the regulation of data security in the commercial sector, the FTC has gradually begun to regulate inadequate data security as an unfair or deceptive practice under section 5 of the FTCA, despite any official grant of such authority in the data security context.[86] The FTC has been successful in its administrative enforcement actions, but it now faces resistance that it did not previously encoun-

81. H.R. 1053, at 16.

82. *See* Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 618 (2015).

83. *See* Maureen K. Ohlhausen, FTC Comm'r, Success in Self-Regulation: Strategies to Bring to the Mobile and Global Era, Address at the BBB Self-Regulation Conference 2–4 (June 24, 2014), https://www.ftc.gov/system/files/documents/public_statements/410391/140624bbbself-regulation.pdf; *see also* Scott, *supra* note 15, at 130 ("By 2000, however, the Commission recognized that industry self-regulation was not working, and that 'substantially greater incentives' would be required to protect consumer privacy online.").

84. Ohlhausen, *supra* note 83, at 2–4.

85. DATA SECURITY UPDATE, *supra* note 28.

86. The FTCA does not expressly list what practices constitute as "unfair" or "deceptive," but rather provides a definition that can be applied to various practices. *See* 15 U.S.C. § 45(a)

ter.[87] Previous enforcement actions resulted in consent orders, which are private settlements that require companies to abide by certain information security procedures and reporting requirements.[88] As the FTC expanded its regulatory scope and pursued companies for inadequate information security measures, two challengers refused to enter a consent order and sought to cast doubt on the FTC's authority.[89]

1. FTC Authority Under the FTCA

The FTC was created in 1914 under the FTCA with the original purpose of preventing "unfair methods of competition in commerce."[90] Over time, the scope of the FTC's authority has expanded.[91] Most significantly, in 1938, Congress amended the FTCA to prohibit "unfair or deceptive acts or practices" in addition to "unfair methods of competition" in order to enable the FTC to protect consumers directly.[92] Congress then passed the 1975 Magnuson-Moss Warranty–Federal Trade Commission Improvement Act (Magnuson-Moss Act), which granted the FTC explicit authority to prescribe rules to define specific acts as unfair or deceptive as well the requirements to prevent such unfair or deceptive acts and practices.[93] However, the procedures to pass trade regulation rules became more complex after the passage of the Federal Trade Commission Improvements Act of 1980.[94] Then, in 1994, Congress restricted the FTC's authority by adding section 45(n) and limiting the FTC's discretion in declaring practices "unfair."[95]

(2012). Accordingly, the FTC does not have express authority to regulate inadequate information security measures as an "unfair" practice. *See id.*

87. *See* Bender, *supra* note 24, at 1675 ("FTC's enforcement of data-security policies under the unfairness prong of the FTC[A] has been met with substantial criticism.").

88. *See* Scott, *supra* note 15, at 133, 143–44 ("Since all of the actions brought to date have quickly settled, no judicial opinions exist on the efficacy or legality of the Commission's actions brought under the unfairness doctrine.").

89. Moncada, *supra* note 31, at 921–24.

90. *About the FTC*, *supra* note 29; *see also The Antitrust Laws*, FTC, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/antitrust-laws (last visited Jan. 15, 2017).

91. *About the FTC*, *supra* note 29.

92. 15 U.S.C. § 45(a) (2012); *see also About the FTC*, *supra* note 29.

93. Pub. L. No. 93-637, 88 Stat. 2193 (1975) (codified as amended at 15 U.S.C. §§ 2301-2312 (2012)).

94. Pub. L. No. 96-252, 94 Stat. 374 (codified as amended in scattered sections of 15 U.S.C.). For a detailed discussion of the difference in the rulemaking procedures, see generally Jeffrey S. Lubbers, *It's Time to Remove the "Mossified" Procedures for FTC Rulemaking*, 83 GEO. WASH. L. REV. 1979 (2015).

95. Federal Trade Commission Act Amendment of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (codified at 15 U.S.C. § 45(n) (2012)).

Congress also enacted legislation that charged the FTC with administering various consumer protection laws,[96] including the Truth in Lending Act, CAN-SPAM Act, Children's Online Privacy Protection Act, Equal Credit Opportunity Act, Fair Credit Reporting Act, Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act.[97]

FTC has broad authority to regulate unfair and deceptive practices under the FTCA.[98] The FTC is "empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[99] To establish liability for unfair practices under section 45(a), the FTC must satisfy the three part test under section 45(n) to determine whether a practice is "unfair."[100] Although the FTC is not explicitly granted the authority to regulate information security, the FTC has interpreted inadequate security measures to fall within the meaning of an unfair practice under sections 45(a) and (n).[101]

The FTC has the power to investigate "the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce."[102] Following an investigation, if the FTC has reason to believe there is a violation, it can issue an administrative complaint.[103] The FTC may also bring suit in a district court to seek a permanent injunction and other equitable relief for Defendants' acts that violate section 45(a).[104]

---

96. *About the FTC*, *supra* note 29.

97. DATA SECURITY UPDATE, *supra* note 28.

98. *See* 15 U.S.C. § 45(a)(2) (2012); *see also* DATA SECURITY UPDATE, *supra* note 28.

99. 15 U.S.C. § 45(a)(2).

100. *Id.* § 45(n). Section 45(n), titled "Standard of proof; public policy consideration," provides as follows:

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

Id.

101. *Id.* § 45(a), (n).

102. 15 U.S.C. § 46(a).

103. *Id.* § 45(b).

104. *See id.* § 53(b); *see also* First Amended Complaint for Injunctive Relief & Other Equitable Relief ¶ 1, FTC v. Wyndham Worldwide Corp., No. CV 12 1365 PHX PGR (D. Ariz. Aug. 9, 2012).

The alternative to administrative or judicial proceedings is to pass a TRR that declares specific acts or practices as unfair, and violation of the rule would constitute an unfair practice in violation of section 45(a)(1).[105] The FTC has authority to promulgate TRRs under section 57a(a).[106] The Magnuson-Moss Act added this section to the FTCA to provide clear statutory authority for the FTC to issue TRRs dealing with unfair or deceptive practices.[107] The FTC has not relied on TRRs and instead focuses its efforts on adjudication.[108]

2. FTC Enforcement Actions in Data Security

The FTC has brought actions concerning a wide range of privacy issues, including "over 130 spam and spyware cases and more than 40 general privacy lawsuits."[109] The FTC then expanded its focus and pursued cases more specific to information security.[110] Between 2002 and 2014, "the FTC has brought over 50 cases against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk."[111] Although the FTC has been successful in its enforcement actions so far, the FTC now faces resistance

---

105. *See* 15 U.S.C. § 57a(a)(1). The provision provides as follows:

> [T]he Commission may prescribe—
>
> (A) interpretive rules and general statements of policy with respect to unfair or deceptive acts or practices in or affecting commerce (within the meaning of section 45(a)(1) of this title), and
>
> (B) rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce (within the meaning of section 45(a)(1) of this title), except that the Commission shall not develop or promulgate any trade rule or regulation with regard to the regulation of the development and utilization of the standards and certification activities pursuant to this section. Rules under this subparagraph may include requirements prescribed for the purpose of preventing such acts or practices.

Id.

106. *See id.*; *see also* Stephanie W. Kanwit, *Rulemaking in the Competition Area—Federal Trade Commission power After the Magnuson-Moss Act*, 1 FED. TRADE COMM'N § 5:7 (2015).

107. *See* 15 U.S.C. § 57a(a); Kanwit, *supra* note 106, § 5:7; *see also* Stephanie W. Kanwit, *Magnuson-Moss Rulemaking—Introduction*, 1 FED. TRADE COMM'N § 6:3 (2015) ("The act gave trade regulation rules an independent statutory basis which they had previously lacked, and also prescribed sanctions for their violation, namely civil penalties aimed at deterrence, and consumer redress.").

108. *See* Hurwitz, *supra* note 26, at 997 (noting that although the FTC has clear rulemaking authority, "the FTC consistently relies on adjudication over rulemaking"); *see also* Lydia B. Parnes & Carol J. Jennings, *Through the Looking Glass: A Perspective on Regulatory Reform at the Federal Trade Commission*, 49 ADMIN. L. REV. 989, 996 (1997) ("Designing industry-wide solutions to problems proved difficult in some areas. As a result, the paradigm shifted. Rulemaking is generally undertaken by the Commission in response to congressional directives.").

109. DATA SECURITY UPDATE, *supra* note 28.

110. *Id.*

111. *Id.*

to its regulation of inadequate information security as an unfair practice.

FTC's regulation of data security as an unfair practice is relatively new, and legal precedent is scarce.[112] Recently, two companies declined to settle FTC's charges and challenged the FTC's regulation of information security procedures as an unfair practice.[113]

a. *FTC v. Wyndham Worldwide Corp.*[114]

The first challenger, Wyndham Worldwide Corp. and three of its subsidiaries (collectively referred to as "Wyndham") challenged the action filed in district court and claimed that the FTC lacked authority to regulate data security as an unfair practice.[115] Wyndham's claims were unsuccessful.[116] In 2012, the FTC issued a complaint against Wyndham in district court against Wyndham seeking permanent injunctive relief and other equitable relief for Wyndham's violation of section 45(a).[117] The FTC alleged that Wyndham "violated both the deception and unfairness prongs of section 5(a) 'in connection with Defendants' failure to maintain reasonable and appropriate data security for consumers' sensitive personal information.'"[118] The FTC alleged that Wyndham engaged in unfair cybersecurity practices that, "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[119]

The charges stemmed from Wyndham's failure to implement "readily available security measures" to safeguard sensitive customer information.[120] Wyndham's property management systems stored "names, home addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes" of the hotel patrons.[121] There were three hacking incidents in 2008 and 2009, none

112. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014) ("Despite over fifteen years of FTC enforcement, there are hardly any judicial decisions to show for it.").

113. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re* LabMD Inc., No. 9357, 2015 FTC LEXIS 272 (F.T.C. Nov. 13, 2015), *vacated*, No. 9357, 2016 FTC LEXIS 128 (F.T.C. July 28, 2016), *judgment entered by* No. 9357, 2016 FTC LEXIS 123 (F.T.C. July 28, 2016), *stay granted*, LabMD, Inc. v. FTC, No. 16-16270-D, 2016 U.S. App. LEXIS 23559 (11th Cir. Nov. 10, 2016); *see also* Moncada, *supra* note 31, at 921–24.

114. 799 F.3d 236.

115. *Id*. at 240.

116. *Id.* at 240–42.

117. *See Wyndham*, 10 F. Supp. 3d at 607.

118. *Id.*

119. *Id.* at 608.

120. *Wyndham*, 799 F.3d at 241.

121. *Id.* at 240.

of which Wyndham addressed with any changes or improvements in the hotel's data security protocols.[122] In all three incidents, hackers gained access to Wyndham's computer systems and collectively "stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges."[123]

During the first breach, in April 2008, hackers gained access to Wyndham's national network through a local network in an Arizona hotel.[124] Hackers then repeatedly guessed user names and passwords until they successfully logged into an administrator account that led to unencrypted information on over 500,000 accounts.[125] The second breach, in March 2009, also occurred as a result of hackers gaining access to the administrative account to steal unencrypted payment card information from more than 50,000 customers.[126] Wyndham discovered malware placed from the previous attack that gave hackers access to Wyndham's systems for approximately two months.[127] The last breach occurred later in 2009, when hackers used the same means to steal payment card information from over 69,000 customers.[128] Wyndham was not alerted about this breach until 2010 when a credit card company received complaints of fraudulent charges from its customers.[129]

Among several deficiencies noted by the FTC, Wyndham allegedly stored payment card information in plain text, failed to employ measures to prevent access to its systems by unauthorized third parties, and did not follow proper response procedures after a hacking incident.[130] Wyndham did not utilize encryption or firewalls and allowed the use of very basic and easily ascertainable administrator credentials.[131] Even after the breach, Wyndham did not review its systems for weaknesses or implement safeguards to prevent future attacks, and such disregard resulted in two additional breaches within the same year.[132] Despite these shortcomings in security, Wyndham chose not to settle the charges and challenged the FTC's authority to regulate data security practices.[133]

---

122. *Id.* at 241.
123. *Id.* at 240–41.
124. *Id.* at 241.
125. *Id.* at 242.
126. *Wyndham*, 799 F.3d at 242.
127. *Id.*
128. *Id.*
129. *Id.*
130. *Id.* at 240–42.
131. *Id.* at 241.
132. *Wyndham*, 799 F.3d at 241.
133. *Id.* at 236, 240–42.

Although most FTC enforcement actions settle prior to any significant litigation,[134] Wyndham moved to dismiss the complaint.[135] In its Rule 12(b)(6) motion to dismiss, Wyndham presented three main arguments: (1) the FTC lacked authority to bring charges for unfair practices related to data security; (2) the FTC did not issue formal trade regulations; and (3) the FTC "allegations are pleaded insufficiently to support either an unfairness or deception claim."[136] The district court denied Wyndham's motion to dismiss, but granted interlocutory appeal and certified two questions of controlling law to the Third Circuit Court of Appeals: (1) whether the FTC can bring an unfairness claim under section 45(a) involving inadequate data security; and (2) whether the FTC must promulgate TRRs before bringing an unfairness claim under section 45(a).[137] The Third Circuit Court affirmed that "unfair" acts can include inadequate data security practices.[138] Wyndham eventually settled FTC's charges and entered a consent order.[139]

Although Wyndham settled, the case yielded the first binding decision in the appellate court affirming the FTC's authority to regulate inadequate information security as an unfair practice.[140] Shortly after *Wyndham*, another company chose to adjudicate and challenged the FTC on the merits of their allegations.

b. *In re LabMD, Inc.*[141]

The second company, LabMD, Inc. (LabMD), challenged the merits of the administrative complaint and argued the FTC failed to prove that LabMD's allegedly inadequate data security constituted an unfair

134. *See* Scott, *supra* note 15, at 143–44.

135. *Wyndham*, 799 F.3d at 242.

136. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014).

137. *Id.* at 636.

138. *Wyndham*, 799 F.3d at 240.

139. Press Release, Fed. Trade Comm'n, Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.

140. *See* Solove & Hartzog, *supra* note 112, at 585; *see also* Scott, *supra* note 15, at 143-44; Thomas O'Toole & Katie W. Johnson, *FTC's Unfairness Authority Upheld in Wyndham Data Security Litigation*, BLOOMBERG BNA (Apr. 14, 2014), https://www.bna.com/ftcs-unfairness-authority-n17179889558/. This case also demonstrates the interplay between the FTC's actions alleging deception and unfairness because facts that support the claim of deception also support the claim of unfairness. *See infra* notes 220–33 and accompanying text.

141. No. 9357, 2015 FTC LEXIS 272 (F.T.C. Nov. 13, 2015), *vacated*, No. 9357, 2016 FTC LEXIS 128 (F.T.C. July 28, 2016), *judgment entered by* No. 9357, 2016 FTC LEXIS 123 (F.T.C. July 28, 2016), *stay granted*, LabMD, Inc. v. FTC, No. 16-16270-D, 2016 U.S. App. LEXIS 23559 (11th Cir. Nov. 10, 2016).

practice within the meaning of the FTCA.[142] The Administrative Law Judge (ALJ) agreed and dismissed the complaint for failure to establish that LabMD's conduct resulted in actual or likely harm to consumers as required by section 45(n).[143] The ALJ's dismissal of the FTC complaint yielded the first successful challenge to the FTC's allegations of inadequate data security based on the merits of the case.[144] The FTC commissioners then issued an opinion reversing the ALJ's decision and concluding that LabMD's data security practices constituted an unfair act or practice within the meaning of section 5 of the FTCA.[145] The order is currently stayed pending LabMD's appeal.[146] The FTC has not faced such adamant opposition in the past.[147] This case identified weaknesses in the FTC's claim, which is premised solely on unfairness and not deception.[148]

On August 28, 2013, the FTC initiated an administrative action against LabMD, a medical testing laboratory.[149] The complaint alleged LabMD's failure to employ "reasonable and appropriate" measures to prevent unauthorized access to consumer's personal information "'caused or is likely to cause' substantial consumer injury."[150] The FTC pointed to two LabMD "security incidents" that resulted from inadequate information security.[151]

The first incident occurred in May 2008 when Triversa Holding Company (Triversa), a "data security company that offers breach detection and remediation services"[152] informed LabMD that it found LabMD's insurance aging report on LimeWire, a peer-to-peer file-sharing network which allowed one computer user to access the files shared by another computer user through the same file-sharing application.[153] The report contained 1718 pages of personal patient information, including names, social security numbers, and medical records of approximately 9300 of LabMD's patients (referred to as the "1718 File").[154] The insurance aging report was shared through LimeWire,

142. *In re LabMD Inc.*, 2015 FTC LEXIS 272, at *5–6.
143. *Id.* at *200–01.
144. *Id.* at *1.
145. *In re LabMD, Inc.*, 2016 FTC LEXIS 128, at *1–2.
146. *LabMD, Inc.*, 2016 U.S. App. LEXIS 23559, at *1–2.
147. *See* Bender, *supra* note 24, at 1675 ("FTC's enforcement of data-security policies under the unfairness prong of the FTC Act has been met with substantial criticism.").
148. *In re LabMD Inc.*, 2015 FTC LEXIS 272, at *1.
149. *Id.*
150. *Id.*
151. *Id.* at *2.
152. *Id.* at *2, *53.
153. *Id.* at *124–25.
154. *In re LabMD Inc.*, 2015 FTC LEXIS 272, at *3.

which was installed on the computer used for billing.[155] Triversa offered its services to LabMD by representing that LabMD's file had spread across the file sharing network and offered its services to mitigate the damage. [156] LabMD investigated the incident, but refused to hire Triversa.[157]

The second incident occurred in October 2012 when the Sacramento California Police Department (SPD) found documents associated with LabMD when they searched a house as part of investigation into utility bill fraud.[158] The officers found forty "Day Sheets" containing names and social security numbers of approximately 600 consumers as well as copies of nine checks made payable to LabMD (collectively referred to as "Sacramento Documents").[159] The Day Sheets are generated through LabMD's billing software.[160] There also were documents containing social security numbers that were used by different people.[161] The individuals in possession of the documents "subsequently pleaded 'no contest' to identity theft charges."[162]

The ALJ dismissed the complaint holding that the FTC did not meet its burden of proof to show that LabMD's "failure to employ reasonable data security constitutes an unfair trade practice" under the FTCA.[163] Specifically, the FTC failed to satisfy the first prong of the three-part test set out in section 45(n) of the FTCA,[164] which limits unfair trade practices to conduct that "causes or is likely to cause substantial injury to consumers."[165] Regarding the first incident, the ALJ found insufficient evidence to conclude that the brief exposure of the 1718 File resulted in any substantial harm.[166] Regarding the Sacramento documents, the ALJ held that there was an insufficient causal connection between the documents and LabMD's failure to reasonably safeguard information contained in its electronic files.[167] In particular, the ALJ pointed to the lack of evidence showing the Sacramento Documents were obtained from LabMD's system.[168] Considering the

155. *Id.* at *50.
156. *Id.* at *62.
157. *Id.* at *52–53.
158. *Id.* at *152.
159. *Id.*
160. *In re LabMD Inc.*, 2015 FTC LEXIS 272, at *157.
161. *Id.* at *3.
162. *Id.* at *108–09.
163. *Id.* at *25–26.
164. *Id.* at *26.
165. 15 U.S.C. § 45(n) (2012).
166. *In re LabMD Inc.*, 2015 FTC LEXIS 272, at *26.
167. *Id.*
168. *Id.* at *26–27.

totality of the presented evidence, the ALJ concluded that the FTC failed to establish substantial consumer injury and dismissed the complaint.[169] The FTC promptly filed a Notice of Appeal to have the FTC commissioners review the decision.[170]

The FTC commissioners reversed the ALJ's decision, concluding that "the ALJ applied the wrong legal standard for unfairness" and that "LabMD's security practices were unreasonable, lacking even basic precautions to protect the sensitive consumer information maintained on its computer system."[171] The FTC issued a final order requiring LabMD to implement certain compliance measures, including a comprehensive information security system.[172] LabMD appealed the Final Order and sought a stay pending review.[173] The Eleventh Circuit Court of Appeals granted the stay, holding that LabMD made a sufficient showing that it is likely to succeed on the merits and that it will be irreparably injured absent a stay.[174] The Eleventh Circuit Court reasoned that "it is not clear that a reasonable interpretation of § 45(n) includes intangible harms like those that the FTC found in this case" and that "it is not clear that the FTC reasonably interpreted 'likely to cause' as that term is used in § 45(n)."[175] The appeal remains to be decided on the merits.

The FTC expended considerable time and resources to prove that a company's inadequate information security program constitutes an unfair practice under the FTCA. As this is still a relatively novel issue, the FTC is likely to face greater resistance in future enforcement actions. Moving forward, case-by-case adjudication is not a practical manner of enforcement.

III. Analysis

Despite the efforts of the judicial, legislative, and administrative bodies, effective information security regulation is still lacking for certain business entities.[176] Although data breaches are not always pre-

169. *Id.* at *200–01.

170. Jessica Corso, *FTC Appeals Unfavorable LabMD Data Breach Decision*, Law360 (Nov. 25, 2015), http://www.law360.com/articles/731601/ftc-appeals-unfavorable-labmd-data-breach-decision.

171. *In re* LabMD, Inc., No. 9357, 2016 FTC LEXIS 128, at *1 (F.T.C. July 28, 2016).

172. *In re* LabMD, Inc., No. 9357, 2016 FTC LEXIS 123, at *1–2 (F.T.C. July 28, 2016).

173. LabMD, Inc. v. FTC, No. 16-16270-D, 2016 U.S. App. LEXIS 23559, at *6 (11th Cir. Nov. 10, 2016).

174. *Id*. at *6–7.

175. *Id*. at *9–10.

176. *See generally* Ieuan Jolly, *Data Protection in United States: Overview*, *in* Data Protection Global Guide, Westlaw (database updated July. 1, 2016), http://us.practicallaw.com/6-

ventable and may occur even with adequate information security measures, certain basic safety measures should be employed by all entities to substantially reduce the risk of a data breach. FTC's strategy to use case-by-case adjudication cannot produce the kind of industry-wide effect necessary to substantially reduce the risk of data breaches.[177] The FTC should issue a TRR that declares a covered entity's failure to implement a reasonable data security program as an unfair practice within the meaning of section 45(n) and prescribes methods that may be implemented by the covered entity as part of a reasonable information security program, which should be tailored to each entity based on the type of data it stores. It is important to note that a data breach in itself is not a per se violation of section 45(a).[178] Instead, a violation occurs when a company fails to implement reasonable security, and such security deficiencies lead to a data breach.[179] If company employed reasonable information security, but still experienced a data breach, then, there is no violation of section 45. A TRR would function in the same manner.

In the fifteen years that the FTC commenced actions arising out of inadequate information security, most of the respondents elected to settle.[180] The two companies who challenged the FTC's claims are the first, but they certainly will not be the last. Resistance to the Commission's regulation of data security is still in the early stages.[181] The FTC cannot effectively regulate data security if it has to establish the elements of an unfair practice under the FTCA in each and every

502-0467 (noting that data breaches continue to plague industries across the United States, even with judicial, legislative, and administrative regulations attempting prevent them).

177. *See* Solove & Hartzog, *supra* note 112, at 585 ("Despite over fifteen years of FTC enforcement, there are hardly any judicial decisions to show for it."); *see also* Scott, *supra* note 15, at 143–44 ("Since all of the actions brought to date have quickly settled, no judicial opinions exist on the efficacy or legality of the Commission's actions brought under the unfairness doctrine.").

178. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 626 (D.N.J. 2014) (concluding that "[t]he FTC therefore does more than simply assert 'that a violation . . . must have occurred simply because the data loss incident occurred.' It alleges insufficiencies that, drawing reasonable inferences in favor of the FTC, led to data-security breaches." (citation omitted) (quoting Willey v. J.P. Morgan Chase, N.A., 2009 U.S. Dist. LEXIS 57826, at *4 (S.D.N.Y. July 7, 2009))); *see also FTC Statement*, *supra* note 15, at 5 ("Although a breach may indicate a problem with a company's security, breaches can happen . . . even when a company has taken every reasonable precaution. In such instances, the breach will not violate the laws that the FTC enforces.").

179. *Wyndham*, 10 F. Supp. 3d at 626.

180. *See* DATA SECURITY UPDATE, *supra* note 28.

181. *See* Bender, *supra* note 24, at 1675; Deborah Gersh et al., *LabMD and FTC's Attempt to Expand Data Security Authority*, LAW360 (Aug. 3, 3016, 5:13 PM), https://www.law360.com/articles/824067/labmd-and-ftc-s-attempt-to-expand-data-security-authority (providing the timeline for the *LabMD* case and the FTC's attempt to expand its authority).

case. The difficulty of establishing the necessary elements makes the outcome of cases uncertain, and individual, fact-intensive proceedings are time consuming. Although the FTC gained much needed judicial affirmation of its authority to regulate data security under the unfairness prong in *Wyndham*, the holding in that case is limited to the Third Circuit and the court merely confirms the FTC's authority to find certain inadequacies in information security as unfair practices.[182] The court reviewed neither the merits of the allegations nor the standards on which the FTC relies.[183] While case-by-case adjudication has worked in the past, moving forward, a TRR would allow the FTC to regulate information security practices much more effectively and efficiently. Section A examines the FTC's power to promulgate TRRs,[184] as compared to the FTC's power to adjudicate and enter into consent orders, as discussed in Section B.[185] Section C analyzes the challenges to FTC's authority to regulate inadequate information security as an unfair practice under section 45(a) of the FTCA.[186] Finally, Section D discusses the difficulties in establishing each element of the test to determine whether a practice is unfair under section 45(n).[187]

A. Trade Regulation Rules

The FTC has the power to promulgate TRRs in addition to enforcing regulations through administrative adjudication.[188] The Magnuson-Moss Act granted the FTC explicit authority to prescribe rules to define specific acts as unfair or deceptive.[189] However, the procedures to pass trade regulation rules became more complex after the passage of the Federal Trade Commission Improvements Act of 1980.[190] There are sixteen TRRs currently in effect, which are codified in 16 C.F.R., subchapter D.[191] Due to the complicated and extensive procedures, no new rulemaking has been initiated since 1980.[192]

182. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 259 (3d Cir. 2015).

183. *See id.* at 236, 252–57.

184. *See supra* notes 188–97 and accompanying text.

185. *See supra* notes 197–232 and accompanying text.

186. *See supra* notes 233–61 and accompanying text.

187. *See supra* notes 261–305 and accompanying text.

188. *See* 15 U.S.C. §§ 45(a), 45(n), 57a (2012); *see also* Hurwitz, *supra* note 26 (noting that although the FTC has clear rulemaking authority, "the FTC consistently relies on adjudication over rulemaking").

189. Pub. L. No. 93-637, 88 Stat. 2193 (1975) (codified as amended at 15 U.S.C. §§ 2301-2312 (2012)).

190. Pub. L. No. 96-252, 94 Stat. 374 (codified as amended in scattered sections of 15 U.S.C.). For a detailed discussion of the rulemaking procedures, see generally Lubbers, *supra* note 94.

191. 16 C.F.R., subch. D (2016).

192. Lubbers, *supra* note 94, at 1989.

In the area of information security, the benefits of a TRR outweigh the cumbersome process required to promulgate it.[193] In the long run, a TRR will be much more effective to regulate data security than a series of administrative proceedings and consent orders. If the FTC passes a TRR that requires certain minimum information security measures, each covered entity will be explicitly required to information security program that is reasonable for its particular circumstances because and failure to comply would be a violation of the TRR and constitute an unfair practice in violation of section 45(a)(1).[194] This TRR would eliminate the respondent's ability to challenge to FTC's authority to regulate inadequate data security as an unfair practice.[195] The TRR would also eliminate FTC's burden to establish all the elements of an unfair practice in each individual proceeding.[196] The issue will not be whether the FTC has authority to regulate inadequate data security as an unfair practice, but rather whether a company's information security program is adequate and reasonable. The FTC could then better allocate its resources to enforce of the TRR and pursue a larger number of noncompliant entities. Given the rising rate of data breach instances in the business sector, pursuing approximately a dozen companies per year as the FTC has done is not efficient and will not bring about market wide change that is necessary to safeguard consumers against unauthorized access to their personal and financial information due to lacking or inadequate data security measures.

B. Administrative Proceedings

A series of administrative actions and consent orders is not an efficient way to effectuate change in the industry. Administrative proceedings yield one of two results: (1) the respondent elects to settle and enters a consent order delineating the required corrective action;[197] or (2) the respondent challenges the charges and goes through the drawn out administrative proceedings.[198]

193. *See* 15 U.S.C. § 57a; *see also* Lubbers, *supra* note 94, at 1982.

194. *See* 15 U.S.C. § 57a.

195. *See, e.g.*, *supra* notes 135–37 and accompanying text.

196. *See* 15 U.S.C. § 57a.

197. *See, e.g.*, DATA SECURITY UPDATE, *supra* note 28.

198. *See, e.g.*, Moncada, *supra* note 31, at 921–24.

1. Consent Orders

If the respondent elects to settle the charges brought by the FTC, the resulting settlement is referred to as a consent order.[199] Consent orders are voluntary settlements between the FTC and the respondent that typically last twenty years and prescribe corrective action as well as compliance and reporting standards that the respondent must abide by during the twenty year period.[200] The scope of the consent order varies in each case and is narrowly tailored to the circumstances in each case.

The benefits to respondents to avoid an administrative proceeding create a strong incentive to settle despite the long time commitment and extensive compliance standards. Administrative adjudication is time-consuming, costly, and unlikely to result in a favorable verdict for the respondent because the reviewing court grants considerable deference to the FTC.[201] Additionally, when a respondent enters into a consent order, the respondent does not admit liability, which is attractive to companies seeking to salvage its reputation.[202]

The FTC has been successful in settling its enforcement actions in data security partly because many of the cases involved claims of a deceptive practice pursuant to section 45(a),[203] which is easier for the FTC to establish than a claim of an unfair practice because deceptive practices are not subject to the requirements of section 45(n) that sets forth a three-part test to determine whether a practice is unfair.[204] The Commission can bring a claim for a deceptive practice when a

199. *See* Solove & Hartzog, *supra* note 112, at 607 ("Technically, consent orders legally function as contracts rather than as binding precedent.").

200. *See* Bender, *supra* note 24, at 1675 ("Generally, these consent orders require the companies to submit periodic independent audit results and other reports indicating compliance with the Commission's data-security standards.").

201. Although LabMD prevailed in the initial administrative action, before the FTC commissioners overturned the ALJ's decision, the financial burden and negative publicity were too great, and the company went out of business during the drawn out proceedings. *See* Dune Lawrence, *A Leak Wounded This Company. Fighting the Feds Finished It Off: Michael Daughtery Learns the High Price of Resistance*, BLOOMBERG BUSINESSWEEK (Apr. 25, 2016), https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/. Perhaps, companies that chose to settle did so to avoid a similar fate.

202. *See* Solove & Hartzog, *supra* note 112, at 610 ("One of the main motivations for settling with the FTC is that it allows the company to avoid admitting wrongdoing in exchange for remedial measures.").

203. *See* 15 U.S.C. § 45(a) (2012).

204. *See* 15 U.S.C. § 45(a), (n); *see also* G.S. Hans, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163, 171 (2012) ("Deception remains the most commonly used prong of the FTC[A]. This is likely because of its relative clarity compared to unfairness—it is easier to identify a discrete example of a deceptive practice that misleads consumers than one that is unfair to consumers.").

company announces its own standard for information security and fails to deliver on that standard.[205] Consumers rely on the company's promise that it will safeguard their personal information, and sometimes even choose one company over another because of that promise. Under the FTCA, a company deceives the customers when it promises certain security but does not implement measures to provide the security it promises.[206]

In many cases, the FTC initiated a claim of deception after a company suffered a data breach that exposed consumer personal and financial information.[207] A data breach itself is not a per se violation of section 45(a), but failing to implement promised security measures can constitute as a deceptive practice because the company deceived the public by not actually proving the security services it promised.[208] In many instances, a data breach serves as an alert that the company may not have adequate information security measures. Data breaches can occur even when a company utilized reasonable security measures; however, promising certain security to consumers and not providing that security is a deceptive practice that is prohibited by section 45(a).[209] In such cases, it was in the respondent's interest to settle and comply with the consent order than risk challenging the allegations because the respondents have a low chance of prevailing.

The result of the FTC's enforcement practice is a collection of voluntary settlements rather than adjudicated cases.[210] The consent orders offer no binding legal precedent for the FTC to rely on in future enforcement actions.[211] The FTC urges companies to look to these consent orders for guidance as to what constitutes reasonable security

205. 15 U.S.C. § 45(a); *see, e.g.*, FTC v. Tashman, 318 F.3d 1273, 1277 (11th Cir. 2003) (holding that in order to establish liability for deceptive practices under section 45(a), the FTC must show: "(1) there was a representation; (2) the representation was likely to mislead customers acting reasonably under the circumstances, and (3) the representation was material").

206. *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Googles Rollout of its Buzz Social Network (Mar. 30, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz [hereinafter FTC Charges Deceptive Privacy Practices]; *see also* DATA SECURITY UPDATE, *supra* note 28. For example, Fandango, LLC settled charges that it "misrepresented the security of its mobile app and failed to secure the transmission of millions of consumers' sensitive personal information from its mobile app." *Id.*

207. Solove & Hartzog, *supra* note 112, at 630.

208. *Id.*; *see also In re* LabMD Inc., No. 9357, 2015 FTC LEXIS 272, at *114 (F.T.C. Nov. 13, 2015).

209. 15 U.S.C. § 45(a); *see also* FTC Charges Deceptive Privacy Practices, *supra* note 206.

210. *See* Solove & Hartzog, *supra* note 112, at 585 ("Despite over fifteen years of FTC enforcement, there are hardly any judicial decisions to show for it.").

211. *See id.* at 607 ("Technically, consent orders legally function as contracts rather than as binding precedent.").

practices; however, this guidance does not have the force of law.[212] Several commentators view the FTC's prior enforcement actions and consent orders as a form of privacy common law that serves as a foundation for a regulatory scheme.[213] Other commentators question whether the FTC's "common law" consisting of consent orders satisfies the constitutionally required fair notice and resembles common law in other legal contexts.[214] In *Wyndham*, the Third Circuit Court reasoned that the previous enforcement action and consent decrees provide fair notice that the FTC may regulate unreasonable data security as an unfair practice,[215] but it does not go as far as to say the previous enforcement actions and consent orders provide notice of the specific requirements for reasonable data security.[216] The Third Circuit Court later commented, in dicta, "the consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a)."[217] The court applied the same reasoning to the guidebooks with suggested information security practices issued by FTC.[218] No other court has determined how much weight to give the consent orders and guidebooks, so it is possible that other courts may disagree with the reasoning of the Third Circuit. Absent a TRR, the FTC faces potential challenges not only to its authority under the FTCA, but also to its reliance on the collection of consent orders and guidebooks as a basis for reasonable information security standards.[219]

---

212. *See* Bender, *supra* note 24, at 1675.

213. *See* Solove & Hartzog, *supra* note 112, at 590; *see also* Gerard M. Stegmaier & Wendell Bartnick, *Another Round in the Chamber: FTC Data Security Requirements and the Fair Notice Doctrine*, 17 J. INTERNET L. 1, 18 (2013).

214. *See* Stegmaier & Bartnick, *supra* note 30, at 674–75.

215. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 257 (3d Cir. 2015).

216. *See id.* at 257 n.22.

217. *Id.*

218. *See id.* at 256 n.21 (noting that "the guidebook could not, on its own, provide 'ascertainable certainty' of the FTC's interpretation of what specific cybersecurity practices fail § 45(n)").

219. Recently, the Commission issued three major publications: (1) the "2014 Privacy and Data Security Update," which provides an overview all of its recent enforcement actions; (2) "Start with Security: A Guide for Business," which lists ten important lessons from the Commission's past enforcement actions; and (3) the "Information Compromise and the Risk of Identity Theft: Guidance for Your Business," which discusses best practices to securely handle information. DATA SECURITY UPDATE, *supra* note 28; *see* FTC, START WITH SECURITY: A GUIDE FOR BUSINESS (2005), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; *see also* FTC FACTS FOR BUSINESS, INFORMATION COMPROMISE AND THE RISK OF IDENTITY THEFT: GUIDANCE FOR YOUR BUSINESS (2015), http://www.consumer.sc.gov/Documents/IDTU/ID%20Theft/ftc_information_compromise.pdf.

2. Administrative Claims Shift from Deceptive to Unfair Practices

When the respondent elects not to settle, the FTC bears a high burden of proof to establish the relevant elements in each and every case, which is very fact intensive and often involves long, drawn out proceedings.[220] As the FTC asserts authority over inadequate information security as an unfair practice without a simultaneous claim of deceptive practices, it will meet greater resistance than it did in the past with claims for deceptive practices because the standard to establish an unfair practice is more specific and the respondent has a great chance of success.

FTC's cases against Wyndham and LabMD reveal the weaknesses in FTC's regulation of inadequate information security as an unfair practice and demonstrate that it is impractical to continue the course of administrative proceedings in lieu of promulgating a TRR. Initially, the FTC started bringing charges for inadequate information security as a deceptive practice, but then the FTC gradually started bringing charges for both unfair and deceptive practices.[221] Unlike FTC's authority to regulate deceptive practices, FTC's power to declare practices unfair is limited by section 45(n).[222] In its suit against Wyndham, the FTC claimed that "Wyndham has published a privacy policy on its website that overstates the company's cybersecurity"[223] and that "Wyndham engaged in unfair cybersecurity practices that, 'taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[224] Although the standards to prove deception and unfairness are different, the Third Circuit Court in *Wyndham* recognized that "analysis of unfairness encompasses some facts relevant to the FTC's deceptive practices claim" and as such, "facts relevant to unfairness and deception claims frequently overlap."[225] Although Wyndham moved to dismiss both the unfair and the deceptive practices claims, the questions certified for interlocutory review only concerned the unfair practices claim.[226]

220. FTC's General Counsel "portrays the unfairness power not as a flexible tool, but as a fuzzy and indistinct doctrine. As he observes, the language of the FTC[A] was intentionally vague in order to allow judicial decisions to further clarify and shape the meanings of deception and unfairness." Hans, *supra* note 204, at 173.

221. *See* DATA SECURITY UPDATE, *supra* note 28.

222. *See* 15 U.S.C. § 45(a), (n) (2012).

223. *Wyndham*, 799 F.3d at 241.

224. *Id.* at 240.

225. *Id.* at 245.

226. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 631 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

The FTC may not have enough to establish that inadequate information security as an unfair practice without facts that typically exist in cases involving deceptive practices. The complaint against LabMD contained allegations of inadequate information security as an unfair practice, but no claims of deceptive practices.[227] The ALJ dismissed the complaint for failure to show that LabMD's data security procedures fell within the scope of unfair practices as set forth by section 45(n).[228] LabMD's success in dismissing the complaint was bittersweet because the drawn out proceedings drove the company out of business.[229] The victory was brief, as the FTC commissioners overturned the ALJ's dismissal and entered judgment against LabMD.[230] LabMD appealed, and the Eleventh Circuit granted a stay pending LabMD's appeal.[231] If there was a TRR, the data security requirements and FTC's authority to enforce them would be more clearly articulated, which would eliminate the kind of needlessly long proceedings that occurred in the LabMD case.[232] Similar challenges to FTC's authority are likely to arise as more companies experience data breaches.

C. Challenges of FTC's Unfairness Authority

The FTC had a successful record of settling its enforcement actions with voluntarily consent orders. Wyndham, however, was not willing to settle like the rest did. Instead, Wyndham claimed that the FTC did not have authority to regulate inadequate data security as an unfair practice. This challenge led to Third Circuit Court affirming FTC's jurisdiction over inadequate data security practices under the FTCA. Although other circuit courts may arrive at a different conclusion, for now, the FTC received much needed affirmation of its regulatory authority.

Wyndham moved to dismiss the FTC complaint for on two grounds relating to FTC's authority under the FTCA: (1) the FTC lacked "authority to assert an unfairness claim in the data security context" and (2) the FTC did not "formally promulgate regulations before bringing its unfairness claim."[233] The threshold issue of authority over unfair

227. *See supra* notes 142–52 and accompanying text.

228. *See supra* notes 163–70 and accompanying text.

229. *See supra* note 201 and accompanying text.

230. No. 9357, 2016 FTC LEXIS 128 (F.T.C. July 28, 2016), *judgment entered by* No. 9357, 2016 FTC LEXIS 123 (F.T.C. July 28, 2016).

231. LabMD, Inc. v. FTC, No. 16-16270-D, 2016 U.S. App. LEXIS 23559 (11th Cir. Nov. 10, 2016).

232. *See* 15 U.S.C. §§ 45(a), 45(n), 57a.

233. *FTC v. Wyndham Worldwide Corp.,* 10 F. Supp. 3d 602, 607 (D.N.J. 2014).

practices in the data context was not adjudicated prior to the *Wyndham* case. As a result, the New Jersey District Court certified an order for interlocutory appeal to the Third Circuit Court to get guidance on the FTC's authority to regulate inadequate data security as an unfair practice.[234] Absent a TRR, FTC's authority to regulate information security practices is unclear. The Third Circuit Court reviewed two main issues: "whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision."[235]

On the issue of data security regulation under the unfairness prong of section 45(a), the Third Circuit Court did not find Wyndham's arguments persuasive.[236] The court issued the first judicial opinion on the scope of FTC's authority under the unfairness prong, which is a significant victory for the FTC because it provided binding precedent, even if it only limited to the Third Circuit. If a company in another circuit similarly challenges the FTC's charges, another court may come to opposite different conclusion, especially if that company had certain data security measures in place, but a breach still occurred. On the second issue, the Third Circuit Court held the FTC did provide sufficient notice that a company could be liable for unfair data security practices under the statute.[237] To remove any uncertainty and prolonged future litigation, the FTC should promulgate a TRR concerning a reasonable minimum standard for information security procedures and foreclose any potential challenges to its authority.

1. Unfairness Claim in the Data Security Context

Wyndham attempted to refute the FTC's charges by focusing on the definition of an unfair practice under the FTCA. The FTCA defines an unfair practice using a multi-factor test, which leaves enough flexibility for the FTC to consider a range of different practices as unfair, but it also creates the possibility for a respondent to argue that a cer-

234. *Id.* at 636. Under 28 U.S.C. § 1292(b), interlocutory appellate review is appropriate when the following three criteria are satisfied:

> When a district judge, in making in a civil action an order not otherwise appealable under this section, shall be of the opinion that such order involves a controlling question of law as to which there is substantial ground for difference of opinion and that an immediate appeal from the order may materially advance the ultimate termination of the litigation, he shall so state in writing in such order.

Id. at 633.

235. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

236. *See supra* notes 113–42 and accompanying text.

237. *Wyndham*, 799 F.3d at 257.

tain practice is not unfair if the FTC fails to establish one of the elements of the definition.

On appeal, Wyndham claimed for the first time that requirements of section 45(n) are "necessary but insufficient conditions of an unfair practice and that the plain meaning of the word 'unfair' imposes independent requirements that are not met."[238] The Third Circuit Court did acknowledge that section 45(n) "may not identify all of the requirements for an unfairness claim" because "it does not answer whether these are the only requirements for a finding of unfairness."[239] The court found the additional requirements proposed by Wyndham inapplicable, and concluded that Wyndham's conduct did not fall outside the scope of the plain meaning of unfair.[240] This interpretation would also be inconsistent with the legislative intent to maintain a limited, yet flexible standard for defining unfair practices.[241] As the court noted, it is doubtful whether a court would impose additional requirements for a practice to constitute as unfair considering the limiting function of section 45(n).[242] While such interpretation is doubtful, it is not impossible, and a different court may come to such a conclusion if the defendant crafts a better argument based on more favorable facts.

Wyndham then argued that "even if cybersecurity were covered by § 45(a) as initially enacted, three legislative acts since the subsection was amended in 1938 have reshaped the provision's meaning to exclude cybersecurity."[243] The Circuit Court did not agree and reasoned that the legislative intervention was only to ease the procedural burden of declaring an act or practice unfair.[244] To the contrary, these legislative acts "expand[ ] the scope of the FTC's authority" beyond the FTCA, rather than define its scope and limitations.[245] Again, a TRR would foreclose this argument by expressly granting authority to the FTC.

Finally, Wyndham argued that "FTC's interpretation of § 45(a) is 'inconsistent with its repeated efforts to obtain from Congress the very authority it purports to wield here.'"[246] Again, the Third Circuit Court disagreed, demonstrating that the FTC's call for Congressional

238. *Id.* at 244.
239. *Id.*
240. *Id.* at 247.
241. *Id.*
242. *Id.*
243. *Wyndham*, 799 F.3d at 247.
244. *Id.* at 248.
245. *Id.*
246. *Id.*

intervention refers to policies to protect consumers beyond the scope of section 45(a).[247] If the FTC promulgates TRRs, respondents would not be able to raise issues of FTC's authority in future enforcement actions, so the FTC can instead use its resources to prove that companies have insufficient data security rather than wasting resources to establish that it can even bring such charges in the first place.[248]

2. Fair Notice in the Data Security Context

Another issue a company may raise in an effort to dismiss the FTC's claims is that the company lacked fair notice that inadequate data security is an unfair practice. Imposing liability under a statute or regulation violates the Due Process Clause of the U.S. Constitution "if the statute or regulation . . . 'fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.' "[249] Absent a TRR, there is no express grant of authority to the FTC to regulate data security practices and no official source that describes the required information security measures, other than the suggestions contained in the guidebooks periodically issued by the FTC.

Wyndham argued that "the FTC failed to give fair notice of the specific cybersecurity standards the company was required to follow."[250] Specifically, "Wyndham argue[d] it was entitled to 'ascertainable certainty' of the FTC's interpretation of what specific cybersecurity practices are required by § 45(a)."[251] The Third Circuit Court held that the previous enforcement actions and consent decrees provide sufficient notice that a company could be liable for unfair data security practices under the statute.[252] The court pointed to Wyndham's own contention that there is no FTC rule that merits deference, so the court is to interpret the meaning of the FTCA, which calls for an "ordinary judicial interpretation of a civil statute, and the ascertainable certainty standard does not apply."[253] Thus, the court ascertained, "The relevant question is not whether Wyndham had fair notice of the *FTC's interpretation* of the statute, but whether Wyndham had fair notice of what the *statute itself* requires."[254] This issue

247. *Id. at* 248–49.
248. 15 U.S.C. § 57a (2012).
249. *Wyndham*, 799 F.3d at 249 (quoting FCC v. Fox Television Stations, Inc., 132 S. Ct. 2307, 2317 (2012)).
250. *Id.*
251. *Id.* at 252.
252. *Id.* at 257.
253. *Id.* at 253.
254. *Id.* at 253–54.

then becomes an as-applied challenge, which is a weak claim. Wyndham is entitled to a very low level of statutory notice because this is a civil statute, not criminal, and does not implicate any Constitutional rights.[255]

For civil statutes regulating economic activities, "a party lacks fair notice when the relevant standard is 'so vague as to be no rule or standard at all.'"[256] The standard for practices that may be found "unfair" under the FTCA is articulated by a three part test set forth in section 45(n).[257] While this standard is not precise, it does provide notice that "the relevant inquiry here is a cost-benefit analysis."[258] An FTC rule that expressly declares inadequate data security as an unfair practice would foreclose such argument and removes the need to make this determination on a case-by-case basis.

In *LabMD*, the ALJ similarly rejected LabMD's contention that it is a violation of Due Process to charge LabMD with utilizing unreasonable data security without first promulgating data security standards.[259] The FTC stated,

> LabMD's due process claim is particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care, and the contexts in which they make those fact-specific judgments are as varied and fast-changing as the world of commerce and technology itself.[260]

Although the FTC is not required to pass a TRR for every unfair trade practice, in a new area such as data security, a TRR would provide much needed clarity and make FTC's enforcement action more streamlined, without prolonged battles over the extent of the FTC's authority.

D. Unfair Practices Under Section 45(n)

The threshold issue of FTC's authority aside, the Commission bears the burden of proof to show that a company's failure to implement reasonable and appropriate security procedures satisfies the elements of an unfair practice.[261] The three part test under section 45(n) provides that the FTC cannot declare an act or practice unfair unless: (1)

---

255. *Wyndham*, 799 F.3d at 255.

256. *Id.* at 250 (quoting CMR D.N. Corp. v. City of Philadelphia, 703 F.3d 612, 632 (3d Cir. 2013)).

257. 15 U.S.C. § 45(n) (2012); *see supra* note 100 and accompanying text.

258. *Wyndham*, 799 F.3d at 255.

259. *In re* LabMD Inc., No. 9357, 2014 FTC LEXIS 2, at *25–26 (F.T.C. Jan. 16, 2014).

260. *Id.* at *47–48.

261. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 610 (D.N.J. 2014).

"the act or practice causes or is likely to cause substantial injury to consumers"; (2) the injury is "not reasonably avoidable by consumers themselves"; and (3) the harm is "not outweighed by countervailing benefits to consumers or to competition."[262] Although the test appears broad enough to encompass inadequate data security as an unfair practice, establishing the elements of the test based on the facts and circumstances of each case is not an easy task for the FTC, as evidenced by the recent case development. A TRR would eliminate the need to establish each element of the test in every enforcement action.

1. Consumer Harm

The first part of the three-part test under section 45(n) provides that the FTC cannot declare an act or practice unfair unless "the act or practice causes or is likely to cause substantial injury to consumers."[263] This part requires a showing of two elements: (i) substantial injury and (ii) causation. In cases of actual harm to consumers, it is easy to establish both elements. Cases involving of "likely" injury are not precluded, but are much tougher to prove.

a. Actual Harm to Consumers

Historically, liability for unfair practices existed only in cases involving actual harm to consumers.[264] In the area of information security, actual harm exists when consumers experience fraudulent charges or identity theft following a data breach. These harms include monetary losses from fraudulent activity and identity theft as well as other costs to remediate credit and monitor for subsequent fraudulent activity.[265]

In *Wyndham*, the FTC sufficiently pled substantial consumer harm because the consumers whose personal and financial information was stolen during the three data breaches at Wyndham suffered actual harm as a result of fraudulent charges and identity theft. The complaint alleged that approximately "619,000 consumer payment card account numbers" were compromised in the three data breaches, resulting in "fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss."[266] Cases involving actual, quantifiable harm do not create any difficulty in establishing substan-

262. 15 U.S.C. § 45(n).
263. *Id.*
264. *In re* LabMD Inc., 2015 FTC LEXIS 272, at *114 (F.T.C. Nov. 13, 2015).
265. *Id.* at *106.
266. *Wyndham*, 10 F. Supp. 3d at 609.

tial harm to consumers because it easily satisfies the test for an unfair practice.[267] A problem arises when actual harm is difficult to prove or when damages are not easily quantifiable, as was the case in *LabMD*. Even if the first two elements are satisfied, failure to establish the last element is fatal to FTC's cause of action.

b. Likely Harm to Consumers

Cases involving potential harm absent any actual harm may not pass the test under section 45(n) because of the ambiguity of the phrase "likely to cause substantial injury."[268] In *LabMD*, the record was devoid of any evidence of actual consumer harm resulting from the two security incidents, so the FTC was required to prove likely harm to consumers.[269] The ALJ pointed out that the FTC could not identify a single consumer who was actually harmed by the alleged unreasonable conduct.[270] In *LabMD*, the parties did not cite "any case where unfair conduct liability has been imposed without proof of actual harm, on the basis of predicted 'likely' harm alone."[271] The FTC did not present any previous case where liability for unfair conduct was imposed absent proof of actual harm.[272] Furthermore, the limited number of enforcement action, all of which resulted in voluntary consent orders, does not give the FTC any binding precedent to back up its allegations.[273] A TRR specifically addressing information security procedures would eliminate the need for this analysis.

The FTC stresses that language of section 45(n) does not require actual harm and that proof of "likely" harm is sufficient. In its complaint against LabMD, the FTC presented four arguments to prove the substantial harm requirement: (1) likely harm from identity theft "based on an 'increased risk' that consumers whose information is exposed in a data breach will suffer identity theft harm"; (2) likely harm from medical identity theft "including monetary losses due to fraudulently procured medical products and services"; (3) "'[s]ignificant risk' of reputational harm, privacy harm, and/or other harms based on stigma or embarrassment"; and (4) "'risk' of harm" to consumers whose information is on LabMD's computer network because the net-

267. 15 U.S.C. § 45(n).

268. *Id*.

269. *In re LabMD Inc.*, 2015 FTC LEXIS 272, at *112.

270. *Id.*

271. *Id.* at *114.

272. *Id.*

273. *See supra* notes 210–14 and accompanying text.

work is at an "increased risk" of a future data breach resulting in identity theft harm, medical harm, and other harms.[274]

The ALJ, however, reasoned that given the length of time that had passed since the incident and the fact that no consumer was actually harmed since two security incidents undermines the FTC's argument that harm is "likely."[275] As there is no definition of "likely" within the statute, the ALJ relied on the plain meaning, which is defined as having a "high probability of occurring or being true."[276] Although the FTC argued that "significant risk" of harm is sufficient to satisfy the first prong, the ALJ reasoned that "significant risk" of harm implies a lower threshold that "likely" harm and is thus insufficient to meet the statutory requirement.[277] The ALJ then concluded that "at best, Complaint Counsel's evidence of 'risk' shows that a future data breach is possible, and that if such possible data breach were to occur, it is possible that identity theft harm would result."[278]

Although the FTC commissioners overturned the ALJ's decision, LabMD is appealing the decision, and the case is stayed pending the appeal.[279] In granting the stay, the Eleventh Circuit Court noted two issues: (1) it is "not clear that a reasonable interpretation of § 45(n) includes intangible harms like those that the FTC found in this case" and (2) "it is not clear that the FTC reasonably interpreted 'likely to cause' as that term is used in § 45(n)."[280] The court stated that this case presents serious legal questions, so it remains to be seen how the Eleventh Circuit will rule.

Considering that the FTC's success in its previous enforcement actions was based on a showing of actual harm, it seems that while a showing of actual harm is not required by statute, it is necessary in order to establish consumer harm. If "likely" harm to consumers is defined as "probable" in the manner the ALJ reasoned, this high burden of proof would be fatal to many cases. In particular, the FTC will have difficulty pursuing companies with unreasonable data security that has not suffered a data breach. As the FTC realized in its administrative action against LabMD, it would be very difficult to prove that

274. *In re LabMD Inc.*, 2015 FTC LEXIS 272, at *110.

275. *Id.* at *112–14.

276. *Id*. at *117 (citing *Likely*, Merriam-Webster, https://www.merriam-webster.com/dictionary/likely (last visited Apr. 19, 2017)).

277. *Id.* at *120.

278. *Id.* at *190.

279. *See In re* LabMD, Inc., No. 9357, 2016 FTC LEXIS 128 (F.T.C. July 28, 2016), *judgment entered by* No. 9357, 2016 FTC LEXIS 123 (F.T.C. July 28, 2016), *stay granted*, LabMD, Inc. v. FTC, No. 16-16270-D, 2016 U.S. App. LEXIS 23559 (11th Cir. Nov. 10, 2016).

280. *LabMD, Inc.*, 2016 U.S. App. LEXIS 23559, at *9–10.

inadequate data security is likely, to "a high probability," to lead to a data breach. Although this inquiry is fact intensive and depends on the circumstances of each case, there may be too many borderline cases which the FTC would not choose to pursue in fear of not meeting the high probability standard. The ALJ referenced the recent Seventh Circuit opinion in *Neiman Marcus*, in which the Third Circuit Court held that "it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach."[281] The court presumed that "the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[282] This high probability standard would effectively confine enforcement action to incidents when there is actual harm because anything less could fall short of the "high probability" standard. Despite the FTC's attempt to distinguish unreasonable data security as an unfair practice separate from occurrences of data breaches, in light of the *LabMD* holding, this effort may be futile.

In the data security context, whether harm to consumers is "likely" is uncertain because once their personal information is accessed, it is purely speculative what happens to it and how consumers are harmed unless there is actual identity theft or fraudulent charges.

c. Causation

The causation element requires a showing that unreasonable data security was the proximate cause of consumer harm. "Proximate cause may be found even where the conduct of the third party is . . . criminal, so long as the conduct was facilitated by the first party and reasonably foreseeable, and some ultimate harm was reasonably foreseeable."[283] This will be of special importance in the near future because as more companies suffer data breaches, it is likely that a consumer's personal information is comprised though various sources. A company could argue that the harm suffered by the consumer is not due to their inadequate security, but rather another company that also suffered a data breach. Although difficult to prove, it could cast doubt on whether a company actually caused or likely caused harm to a consumer by failing to employ a reasonable data security policy. Again, a TRR that clearly articulates the FTC's authority to regulate

281. *In re LabMD, Inc.*, 2016 FTC LEXIS 128, at *134 (quoting Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015)).

282. *Remijas*, 794 F.3d at 693 ("Why else would hackers break into a store's database and steal consumers' private information?").

283. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 246 (3d Cir. 2015) (quoting Westfarm Assocs. v. Wash. Suburban Sanitary Comm'n, 66 F.3d 669, 688 (4th Cir. 1995)).

inadequate data security would eliminate the need to establish each element of an "unfair" practice.

When there is actual harm to consumers in the form In *Wyndham*, the New Jersey District Court held that "FTC's allegations also permit the Court to reasonably infer that Hotels and Resorts' data-security practices *caused* theft of personal data, which ultimately *caused* substantial injury to consumers."[284] Given the severity and frequency of the data breaches, the court noted, "[f]or good reason, Wyndham does not argue that the cybersecurity intrusions were unforeseeable. That would be particularly implausible as to the second and third attacks."[285]

In *LabMD*, the ALJ refused to infer a connection between the Sacramento Documents and any alleged information security shortfalls. There was no evidence that the Day Sheets and checks copies found in Sacramento "had been scanned and archived, or otherwise saved, onto LabMD's computer network."[286] Provided that the billing application generating the Day Sheets does not save an electronic copy after printing the Day Sheet and the fact that LabMD did not implement file scanning and electronic archiving until after the Sacramento incident, it was not plausible to establish causation.[287] In fact, the FTC even "admits that 'there is no conclusive explanation of how LabMD Day Sheets were exposed.'"[288]

The fact pattern in *LabMD* is unique as there was no data breach of the company network, and neither party could ascertain the source of exposure.[289] The holding on this issue should not negatively impact future cases because this fact pattern is unique to this case and the circumstances surrounding discovery of the Sacramento Documents are unlikely to repeat. A TRR would eliminate the need for this kind of fact-intensive inquiry, much like the element that the harm was not avoidable by the consumers.

2. Injury Not Avoidable by Consumers

The determination whether a consumer injury was reasonably avoidable by consumers themselves is fact-dependent.[290] In *Wyndham*, the court held that it cannot declare as a matter of law that con-

284. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 624 (D.N.J. 2014).
285. *Wyndham*, 799 F.3d at 246.
286. *In re* LabMD Inc., No. 9357, 2015 FTC LEXIS 272, at *157 (F.T.C. Nov. 13, 2015).
287. *Id.*
288. *Id.* at *160.
289. *See id.* at *157–60.
290. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 625 (D.N.J. 2014).

sumers can avoid injury from payment cards.[291] The court referenced precedent and agreed that "unrebutted evidence supports a finding that the harm suffered by consumers was not reasonably avoidable."[292] In *LabMD*, the court did not make further inquiry into the remaining two prongs because the FTC failed to establish the first prong under section 45(n).[293]

3. Harm Is Not Outweighed by Benefits

The second prong of the test under section 45(n) is that the injury is "not reasonably avoidable by consumers themselves"[294] This portion is a cost-benefit analysis which considers the trade-offs of the practice.[295] An act or practice is not unfair "unless it is injurious in its net effects."[296]

Wyndham did not present any arguments for not meeting last prong under section 45(n).[297] In *LabMD*, again, because the FTC provided insufficient proof to establish the first prong under section 45(n), the court did not make further inquiry into the remaining two prongs.[298]

4. Reasonable Data Security

An issue that is yet to be adjudicated on the merits is a company's failure to implement reasonable and appropriate data security.[299] In *Wyndham*, the parties settled out of court before the case was decided on the merits.[300] In *LabMD*, the ALJ did not need to address this question,[301] and FTC's failure to satisfy the requirements of section 45(n) was "fatal to its case."[302] The inquiry into LabMD's data secur-

---

291. *Id.*

292. *Id.* (quoting FTC v. Inc21.com, 745 F. Supp. 2d 975, 1004 (N.D. Cal. 2010)).

293. *In re LabMD Inc.*, 2015 FTC LEXIS 272, at *192.

294. 15 U.S.C. § 45(n) (2012).

295. *See* Scott, *supra* note 15, at 159.

296. *Id.* (quoting *In re* Int'l Harvester Co., 104 F.T.C. 949, 1073 (1984)).

297. *See generally* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

298. *In re LabMD Inc.*, 2015 FTC LEXIS 272, at *192.

299. *See Wyndham*, 799 F.3d at 256 (noting that "we leave for another day whether Wyndham's alleged cybersecurity practices do in fact fail").

300. Press Release, Fed. Trade Comm'n, Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information at Risk (Dec. 9, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.

301. Administrative Judge Chappell concluded that "[b]ecause the evidence fails to prove that Respondent's *alleged unreasonable data security* caused, or is likely to cause, substantial consumer injury, as required by section 5(n) of the FTC[A], Respondent's *alleged unreasonable data security* cannot properly be declared an unfair act or practice in violation of section 5(a) of the FTC[A]." *In re LabMD Inc.*, 2015 FTC LEXIS 272, at *192-93 (emphasis added).

302. *Id*. at *121. ALJ Chappell concluded that "[b]ecause the evidence fails to prove that Respondent's *alleged unreasonable data security* caused, or is likely to cause, substantial con-

ity ended there, and LabMD's unreasonable conduct remained referenced as "alleged."[303]

Furthermore, in *LabMD*, the ALJ stated that the FTC "referred to negligence standards as relevant to the 'unreasonable data security' claim."[304] In the FTC's order denying LabMD's motion to dismiss, the FTC argues that an amorphous reasonableness standard is not unique to data security, but is actually the norm in tort liability.[305]

IV. IMPACT

The FTC's current approach to data security regulation cannot address the issue of the escalating occurrences of data breaches. As demonstrated in *Wyndham* and *LabMD*, FTC's unfairness authority can be challenged on many different grounds.[306] Therefore, it is only a matter of time before companies charged with allegedly unreasonable information security challenge that standard as well. Proving that a company utilized unreasonable data security is the final hurdle. So far, the FTC has pursued companies that either lacked data security procedures altogether or procedures in place were obviously inadequate, similar to *Wyndham*.[307] In such cases, the companies could not easily contest the FTC's allegations and chose to settle.[308] Due to the high cost and negative publicity associated with mitigating damage caused by a data breach, many companies implement some form of improved information security procedures, which may or may not be up to the FTC's standards.[309] When this occurs, the FTC will likely face stronger opposition, as companies will have grounds to challenge their compliance with the amorphous reasonableness standard.

---

sumer injury, as required by section 5(n) of the FTC[A], Respondent's *alleged unreasonable data security* cannot properly be declared an unfair act or practice in violation of section 5(a) of the FTC[A]." *Id*. at *192–93 (emphasis added). Similarly, the Administrative Judge did not address the second and third prongs of the three-part test under section 45(n). *Id*.

303. *Id.* The Administrative Judge also enclosed the word "reasonable" in quotation marks when referring to "reasonable" security. *Id.* at *100 ("Respondent failed to provide 'reasonable' security for Personal Information on its computer networks.").

304. *Id*. at *185 n. 44.

305. *In re* LabMD, Inc., No. 9357, 2014 LEXIS 2, at *47–48 (F.T.C. Jan. 16, 2014) (arguing that "courts and juries subject companies to tort liability for violating uncodified standards of care, and the contexts in which they make those fact-specific judgments are as varied and fast-changing as the world of commerce and technology itself").

306. *See supra* notes 115-71 and accompanying text.

307. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 609 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

308. DATA SECURITY UPDATE, *supra* note 28.

309. Robert O. Carr, *Small to Mid Size Businesses: The New Target for Hackers*, HEARTLAND BLOG (Feb. 23, 2015), https://www.heartlandpaymentsystems.com/blog/2015/02/23/small-to-mid-size-businesses-the-new-target-for-hackers.

FTC Chairwoman Edith Ramirez issued the following statement following the *Wyndham* decision:

> Today's Third Circuit Court of Appeals decision reaffirms the FTC's authority to hold companies accountable for failing to safeguard consumer data. It is not only appropriate, but critical, that the FTC has the ability to take action on behalf of consumers when companies fail to take reasonable steps to secure sensitive consumer information.[310]

The Chairwoman's statement conveys the FTC's goal to pursue companies that fail to implement a reasonable security program. FTC's resistance to promulgating a TRR is inconsistent with this goal.[311] As demonstrated by *Wyndham* and *LabMD*, pursuing companies under section 45(a) requires the FTC to establish all the elements of an unfair practice while addressing challenges to its authority to bring an unfairness claim in the data security context. The FTC can avoid the uncertain and drawn out proceedings by passing a TRR that specifically proclaims inadequate data security as an unfair practice and prescribes the security measures that could be part of a reasonable security program. Prescribing the standards for security is no longer as daunting because the FTC has already articulated these standards in its consent orders and guidebooks.

Although the FTC has been hesitant to issue a TRR in fear of it being too limiting in scope,[312] the current approach will harm the FTC's ability to successfully bring actions in the future. A TRR is specific in nature, so any form of articulated standard for a reasonable data security means it could quickly become outdated. There are, however, certain basic preventive measures that every company should employ in order to safeguard consumer information. When the methods prescribed in the TRR become outdated or inadequate, the FTC can issue an amendment or a supplement to align the standard with industry best practices at that time.

By refusing to promulgate TRRs that would apply to the commercial sector generally, the FTC is severely limiting its authority to regulate commercial data security, which conflicts with its own mission statement. The FTC proclaimed its mission is to "prevent business

---

310. Press Release, Fed. Trade Comm'n, Statement from FTC Chairwoman Edith Ramirez on Appellate Ruling in the Wyndham Hotels and Resorts Matter (Aug. 24, 2015), https://www.ftc.gov/news-events/press-releases/2015/08/statement-ftc-chairwoman-edith-ramirez-appellate-ruling-wyndham.

311. However, "[i]t is not surprising that administrative agencies generally prefer broader and more discretionary standards to the strictures that defined rules impose." J. Howard Beales, III, *Brightening the Lines: The Use of Policy Statements at the Federal Trade Commission*, 72 ANTITRUST L.J. 1057, 1059 (2005).

312. *See* Hans, *supra* note 204, at 173.

practices that are anticompetitive or deceptive or unfair to consumers . . . without unduly burdening legitimate business activity."[313] Adjudicating on a case-by-case basis is not an efficient way for the FTC to protect consumers from harm due to inadequate information security. If the goal is to prevent harm before it occurs, a dozen enforcement actions every year is not the way to achieve that goal. With a few exceptions, once a company experiences a data breach, it takes steps to improve its information security procedures.[314] In response to the escalating instances of data breaches, the business sector will eventually self-regulate until businesses employ some form of a data security program.[315] At that point, however, the damage will already be done.

Until recently, the targets were major retailers and large financial institutions where hackers could gain access to a large volume of data in one attack.[316] The companies naturally responded by promptly improving security practices because larger companies have available resources to overhaul their information security practices. This change in the larger corporations is expected because their breaches are highly publicized, and the company needs to salvage its reputation and retain customers. As larger companies employed better security practices, hackers shifted focus to smaller companies, which are not as well protected and thus more vulnerable.[317] In its 2014 Year-End Economic Report, the National Small Business Association "found that half of all small businesses report they have been the victim of a cyber-attack."[318] The FTC recognized this trend and issued guidebooks and suggested best practices tailored to small and medium sized companies, which may not have an IT department to determine the sufficient security measures.[319] Hackers have shifted focus to smaller companies because although they obtain fewer records per hack, the security system may not be as advanced. The FTC must utilize a broad enforcement approach to counter the prevalent threat of data breaches.

Since the FTC became involved in the regulation of data security practices in 2002, the criticism was the lack of relevant guidelines and

313. *About the FTC*, *supra* note 29.

314. DATA SECURITY UPDATE, *supra* note 28.

315. Carr, *supra* note 309.

316. *Id.*

317. *Id.*

318. NAT'L SMALL BUS. ASS'N, 2014 YEAR-END ECONOMIC REPORT 2 (2015), http://www.nsba.biz/wp-content/uploads/2015/02/Year-End-Economic-Report-2014.pdf. The 2014 Year-End Economic Report was among 675 small business owners across every industry in every state in the nation. *Id.*

319. *Data Security*, FTC, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security (last visited Apr. 19, 2017).

suggested practices that left companies in the dark about what they are required to comply with.[320] In response to this critique, the FTC has released numerous guides that recommend best practices for business.[321] Though well intentioned and necessary—these guides do shed some light on what the FTC expects—the necessary security standard is still vague.[322] The FTC casts a wide net and suggests different practices that may contribute to reasonable security.[323] Businesses are left to reconcile all of these sources and come up with a "reasonable" combination.[324] The guides can be consolidated to serve as foundation for a TRR, which may prescribe the particular means by which companies can avoid committing unfair acts.[325] The FTC has already dedicated so much effort to research, enforcement, and education about reasonable information security practices, so it has the necessary resources to pass a TRR.[326]

V. Conclusion

As technology develops and people utilize more internet connected devices, the volume of generated data continues to climb to unprecedented levels. As more data is being generated, more personal and financial information is collected and stored by entities across different industries. Individuals generally have no control over where or how their personal information is stored; therefore, it is up to the government to act on behalf of the people to protect their personal information. In the area of commerce, the FTC has taken a leading role to protect consumers from substantial injury due to unfair and deceptive data security practices. The effort, while much needed, is becoming futile in light of the escalating data breaches.

The FTC must reconsider its enforcement to devise a more efficient, broader approach, which can be made possible by promulgating TRRs. The FTC has been reluctant to pass TRRs in fear of the rules being too limiting and becoming obsolete as technology rapidly evolves. While it is unlikely the FTC will change its enforcement approach in the near future, as data breaches continue, perhaps it will see the urgency in reconsidering its position. Despite cumbersome

320. Stegmaier & Bartnick, *supra* note 30, at 691.

321. *Data Security*, *supra* note 319.

322. *See supra* note 219 and accompanying text.

323. *Data Security*, *supra* note 319.

324. *Id.*

325. *See* 15 U.S.C. § 57a(a).

326. *See* Data Security Update, *supra* note 28. The FTC has invested in public education and has "hosted over 35 workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security" beginning in 1996. *Id.*

procedure, the FTC should utilize its authority to promulgate TRRs to regulate inadequate data security programs as an unfair practice.

*Nelly Rosenberg**

* J.D. Candidate, DePaul University College of Law, 2017. Thank you to my family and friends for their constant support and endless encouragement. Special thanks to my editors Wei Chen Lin and Riebana Sachs for their guidance and helping me complete this Comment. I would also like to thank my fellow editors and staff of Volume 66 for all their hard work. All mistakes are, of course, my own.